SEPTEMBER 2022

COMMERCIAL VIRTUAL HEALTHCARE SERVICES IN CANADA: DIGITAL TRAILS, DE-IDENTIFIED DATA AND PRIVACY IMPLICATIONS

SHERYL SPITHOFF, BRENDA MCPHAIL, QUINN GRUNDY, LESLIE VESELY, ROBYN K. ROWE, MATTHEW HERDER, BÉATRICE ALLARD AND LESLIE SCHUMACHER

VERSION 2.0

COMMERCIAL VIRTUAL HEALTHCARE SERVICES IN CANADA: DIGITAL TRAILS, DE-IDENTIFIED DATA AND PRIVACY IMPLICATIONS

This report can be downloaded from: http://www.healthtechandsocietylab.org/

Cite as: Spithoff, S., McPhail, B., Grundy, Q., Vesely, L., Rowe, R.K., Herder, M., Allard, B., & Schumacher, L. (2022). "Commercial virtual healthcare services in Canada: Digital trails, de-identified data and privacy implications." Health Tech and Society Lab. Toronto.

Affiliations:
Sheryl Spithoff, University of Toronto and Women's College Hospital
Brenda McPhail, Canadian Civil Liberties Association
Quinn Grundy, University of Toronto
Robyn K. Rowe, Health Data Research Network Canada and Institute for Clinical Evaluative Sciences (ICES)
Matthew Herder, Dalhousie University

Health Tech and Society Lab
76 Grenville Street, Toronto, ON
leslie.vesely@wchospital.ca
http://www.healthtechandsocietylab.org/

We would like to thank Lana Mogic for her research assistance. We thank Owen Adams, Erica McLachlan, and Jay Shaw for their feedback. Additionally, we thank the participants who joined this project's dissemination meeting and the participants who attended our presentation at the 2022 International Association of Privacy Professional's Canada Privacy Symposium. We thank all attendees for their thoughtful feedback and insights.

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC) through their Contributions Program; the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

BLOOMBERG LAWRENCE S. BLOOMBERG FACULTY OF NURSING UNIVERSITY OF TORONTO

CANADIAN CIVIL LIBERTIES ASSOCIATION / ASSOCIATION CANADIENNE DES LIBERTES CIVILES

WCH WOMEN'S COLLEGE HOSPITAL

Family & Community Medicine UNIVERSITY OF TORONTO

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In this analysis, we explored the privacy implications of the direct-to-patient commercial virtual care platforms (VCPs) in Canada. We defined a commercial VCP as a proprietary platform owned by a for-profit company that offers virtual physician or nurse practitioner healthcare services directly to patients through a phone application (app) or website. The use of these commercial VCPs in Canada exploded with the Covid-19 pandemic, transforming access and care, as well as raising concerns about the privacy of health data.

We identified 61 commercial VCPs owned by 54 companies operating in Canada. VCP companies were largely privately held (49/54, 91%) and based in Canada (94%). Most of the platforms offered primary care services (46/61, 75%) and 15 (25%) provided only specialized services, such as pediatric, psychiatric, dermatology, and HIV prevention services. We interviewed 18 key informants affiliated with 12 different companies between October 2021 and January 2022. Nine participants were employees of companies with VCPs and nine were individuals who had affiliations with the industry as consultants, academic researchers, or third-party subcontractors. We also collected 30 documents from the 54 VCP companies and included 10 in our analysis. We conducted primary legal research based on the federal and provincial privacy legislation relating to personal health information (PHI), with a primary focus on Alberta and Ontario, as examples of provincial health information acts. For our secondary legal research, we analyzed relevant articles, bulletins, and interpretations of the various privacy legislations as they relate to commercial VCPs. We analyzed research in other jurisdictions that provided examples of more robust privacy protections. Additionally, we consulted officers in the Offices of the Information and Privacy Commissioners (OIPC) of Ontario and Alberta, as well as the Office of the Privacy Commissioner of Canada (OPC) via informal telephone interviews.

Key findings

- Widespread collection, use and sharing of data
  - Many VCP companies appear to engage in widespread collection, commercial use and, in some cases, sharing of sign-up/registration information (e.g., names, email addresses) and other identifying information (e.g., IP addresses) collected as patients interact with the commercial VCP. Companies often excluded these data from the PHI category, categorizing the data instead as personal information or user data. Excluding these data collected in the context of a health service from the category of PHI creates privacy risks for individuals.
  - These data practices may be particularly problematic if the commercial VCPs only provide one type of health service (e.g., psychiatric services or HIV prevention services) as the information can reveal the nature of a patient's health concern.
  - Some VCP companies also create, use, and share de-identified health information. Research shows these data practices may expose patients to harm from privacy loss, micro-targeting for commercial gain, and discrimination against marginalized individuals and communities. However, federal and provincial legislation provide few protections for de-identified data.
  - The patient datasets include information from First Nations, Inuit, and Métis people in Canada, identifiable by postal code or geolocation codes.

- Consent
  - VCP company privacy policies and terms of service documents are confusing, vague and do not adequately convey how data might be used internally or by third parties.
  - Patients, and clinicians who use the commercial VCPs to provide health services, may not understand how data are being collected and used.
  - Many commercial VCPs appear to require patients to agree to commercial uses of their data prior to accessing health services. Due to jurisdictional complexity, and a lack of guidance, it is unclear if this practice is within the letter of the law, but it is ethically questionable given the sensitivity of a patient/health care system interaction.

- Patient care journeys
  - Some VCP companies use data to influence patient health care journeys, with the goal of optimizing uptake of a business partner's products (e.g., medications or vaccinations). This may affect quality of care and cause harms to patients.

- Public goods
  - As VCP companies view patient data as a proprietary asset, data may not be available to public and non-profit entities for research and health system improvement.

The commercial virtual care industry, therefore, has business practices that pose privacy-related risks. Current oversight and monitoring of these services appears to be impaired by gaps in legislation, unclear legislation, complex jurisdiction and infrequent audits. Harms from these uses of data are likely to fall disproportionately on groups that are marginalized. Changes to legislation, regulation and regulatory practices may reduce the risk of harms. If the commercial virtual care industry, however, cannot survive without monetizing data in ways that expose people to harms, public or non-profit models may be more appropriate.

Recommendations

We recommend that policymakers and regulators find mechanisms to better protect patient privacy when they interact with commercial VCPs. They should clarify jurisdictional issues and increase protections for PHI under the Personal Information Protection and Electronic Documents Act (PIPEDA). They should also bring de-identified health information within the scope of federal and provincial legislation and give it appropriate protections. We recommend that federal and provincial regulators clearly categorize the personal information collected by commercial VCPs as PHI. Additionally, policymakers should ensure that all new and updated legislation recognizes Indigenous data sovereignty. Policymakers and regulators should also ensure that patients can access health services provided by commercial VCPs without having to agree to commercial uses of their data. To ensure quality of care, policymakers should prohibit VCP companies from using platforms to promote pharmaceutical products. Additionally, privacy regulators should regularly audit companies with VCPs. Governments should provide the funding. Regulatory colleges should provide guidance to, and monitor, members (physicians and nurse practitioners) who use the platforms to provide medical services. With respect to the health systems, policymakers should require commercial VCPs to share their data with public entities and Indigenous organizations for research and health system improvement when appropriate. Governments should create infrastructure to facilitate the data-sharing with appropriate data protection. Provincial health systems should ensure that all patients have access to a primary care provider and create mechanisms to promote the integration of virtual care into ongoing care.

SECTION 1: BACKGROUND AND STUDY OBJECTIVE

INTRODUCTION

Prior to the Covid-19 pandemic, the Canadian healthcare system had been slow to adopt virtual care[1] (Box 1). Although most Canadian provinces offered funded virtual healthcare services through their telemedicine networks, they mainly served patients living in rural, remote and Northern communities[2]. As a result, in 2014, virtual care represented only 0.15% of all billable healthcare services[3]. In contrast, in 2016, over half of consultations through the American Kaiser Permanente's integrated health network (the largest in the US) were done virtually[4]. Barriers to broader uptake in Canada included unclear governance, lack of compensation mechanisms, complicated provider licensing requirements, lack of digital interoperability, and privacy concerns[2,5].

In the void of publicly funded models, direct-to-patient commercial VCPs emerged in response to public demand[6,7]. The demand appeared to be driven by poor access to primary care (shortage of family physicians, long wait times for appointments) and increasing interest in virtual care services[8,9]. The commercial VCPs typically offered patients rapid access to appointments with physicians, nurses, and allied health professionals. Prior to the start of the Covid-19 pandemic in Canada, these services were covered by either employee health benefit plans[10] or user fees[7]. The commercial virtual care services provided mostly acute, non-emergency primary care services, chronic care, sexual and mental health care, medical advice, and medication prescription and renewal services[8].

Box 1: Definitions

	Term	Definition
Services	Virtual care (Telemedicine)	Any interaction between patients and/or members of their circle of care (e.g., physicians, nurses), occurring remotely, using any forms of communication or information technologies with the aim of facilitating or maximizing the quality and effectiveness of patient care[11].
Entities	Agent or affiliate of a health data custodian	Acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian. This definition is informed by PHIPA[12] and HIA[13].
	Commerical VCP	A proprietary platform owned by a for-profit company that offers virtual physician or nurse practitioner healthcare services directly to patients through a phone application (app) or website.
	Data brokers, data aggregators, data intensive companies	Companies who aggregate, analyze and monetize personal information.
	Direct-to-patient VCP	Virtual care platform directly accessible to the general public.
	Enterprise VCP	Virtual care platform provided by an employer.
	Health data custodian	An organization or individual with control over personal health information (e.g., physicians, pharmacists, insurance companies, hospitals).
Consent	Express consent	Consent where an individual was presented with clear options to accept or reject giving consent for the collection, use and disclosure of their personal information.
	Implied consent	Consent inferred by an individual's actions and circumstances.
	Meaningful consent	Consent is meaningful and the elements of consent are established, meaning (a) the individual consented or if the individual is incapable of consenting, their substitute decision maker consented; (b) the individual understands what they are consenting to and the consequences of consenting; (c) consent is freely obtained without deception or coercion. This definition is informed by PHIPA[14].
	Valid consent	Consent is valid when an individual is likely to understand the nature, purpose and consequences of the collection, use or disclosure of the personal information. This definition is informed by PEPIDA [15].
Data Types	Aggregated data	Dataset in which one record represents a summary of multiple individuals.
	User data	Data collected as individual conducts online activities (e.g., IP address, device identifiers, geolocation information, etc.).
	De-identified information	Information that cannot be used to identify an individual in reasonably foreseeable circumstances, alone or in combination with other information.
	Personal Health Information	A subset of personal information that pertains to health.
	Personal Information	Information about an identifiable individual.

HIA = Health Information Act; IP = Internet Protocol; PEPIDA = Personal Information Protection and Electronic Documents Act PHIPA = Personal Health Information Protection Act; VCP = Virtual Care Platform

BACKGROUND

Unsurprisingly, the use of virtual care services exploded with the Covid-19 pandemic[9] as patients and providers sought to avoid in person care and provinces introduced funding for virtual care visits. Ontario, for example, saw a 56-fold increase in virtual care visits from 2019 to 2020[16]. Most of these visits appear to be through clinician-initiated virtual care (often a phone call) but some are via direct-to-patient commercial VCPs[17]. The provinces of Ontario, Alberta, and British Columbia provide coverage for direct-to-patient virtual care, while others only fund virtual care when a patient is accessing their regular provider through clinician-initiated virtual care[18]. Some provinces also provide funding for direct-to-patient virtual care when a patient does not have a primary care provider[19].

Commercial VCPs enable convenient and rapid access to primary and specialized healthcare. However, there are also risks associated with the use of commercial VCPs, including poor continuity of care and incomplete diagnosis and treatment[6,7,10,18]. A task force commissioned by the Canadian Medical Association highlighted another concern: the security and privacy of PHI — information about an identifiable individual's mental or physical health[20]. The task force recommended the creation of a pan-Canadian governance structure for virtual care services with policies that ensure patient privacy and confidentiality through secure communications, data access, and data storage.

In addition to PHI, commercial VCPs may also collect other forms of data. One is user data, a seemingly insignificant source of data collected as people browse the internet, use search engines and mobile health apps, and post on social media[21]. This user information often includes internet protocol (IP) address, device identifiers, time of access, browsing history, geolocation information and other identifiers[22]. To gain insights on website users, companies may share these data with third party data brokers (Box 1), for data analytics. Data brokers are part of a complex industry of companies that aggregate, analyze and monetize personal information[22,23]. These include large platforms like Google, Facebook and Amazon, data management and marketing companies like Acixiom, and companies involved in risk analysis like Equifax and Transunion.

VCP companies may also create, use and share de-identified health information. De-identified health information is created by removing key identifiers like name and address from PHI, as well as masking or manipulating quasi-identifiers like date of birth, to ensure the risk of re-identification is low[24]. These data are often regarded as exempt from privacy laws and thus used by VCP companies for a variety of reasons including marketing and analytics[25,26]. De-identified data, however, remains at risk of being deliberately or inadvertently re-identified, which can lead to privacy loss[27]. Even without privacy loss, uses of these forms of data can cause harms from problematic uses of data such as for microtargeting for commercial or political gain, or from the creation of biased algorithms[28,29].

Research indicates that patients do not endorse commercial uses of their data. Systematic reviews[30–32] and a recent Canadian focus group study[33] demonstrated that individuals have low levels of support for commercial use of their health data, de-identified or not. They have concerns about privacy and are worried that profit is the primary motivator. In these situations, study participants want more control over their data, including explicit opt-in consent, as well as assurances that privacy will be protected, and the data will be used for public benefit. In contrast, study participants reported high levels of support for secondary uses of patient data when collected by a trusted academic or non-profit research organization for public benefit. Importantly, groups that have experienced social exclusion — racialized groups, LGBTQ2S+ populations, women, and individuals with lower socioeconomic status — appear to be less comfortable with sharing health data for secondary purposes[31,32]. This may be related to past (and ongoing) exploitation of their data and heightened repercussions from privacy loss.

Commercial VCPs, therefore, are transforming access and disrupting continuity of care, but the platforms may also present privacy related risks from the collection, use, and sharing of health data. Our research goal, therefore, was to describe, analyze and critique the collection and use of health data, from user data to de-identified health information by commercial VCPs in Canada, as well as understand the privacy-related ethical concerns and implications for individuals, communities, marginalized groups, and the broader society.

RESEARCH GOALS

This study aimed to:

1. Describe in detail the entities involved in the commercial provision of virtual care in Canada: platforms, technological innovations, company structure, data-sharing policies, privacy policies, consent procedures, and commercialization of health data.
2. Describe collection and use of data, including how it fits within legal and policy frameworks and the Canadian healthcare system.
3. Examine the privacy-related ethical concerns and implications for individuals, society, diverse groups, and communities.
4. Create recommendations for change.

References

1. NHS Digital. Appointments in General Practice, April 2019. In: NHS Digital [Internet]. Apr 2019 [cited 28 Jan 2021]. Available from: https://digital.nhs.uk/data-and-information/publications/statistical/appointments-in-general-practice/april-2019
2. Canadian Partnership Against Cancer. Virtual care in Canada: Environmental scan. 2019. Available from: https://www.partnershipagainstcancer.ca/topics/virtual-care-canada/
3. Digital Health Canada. Canadian Telehealth Report. 2015. Available from: https://digitalhealthcanada.com/publications/canadian-telehealth-report-2015/
4. Kaiser Permanente. The future of care delivered today. 2018. Available from: https://permanente.org/wp-content/uploads/2018/10/Fact-Sheet_Telehealth_2018.pdf
5. CMA. Virtual care in Canada: Discussion paper. 2019. Available from: https://www.cma.ca/sites/default/files/pdf/News/Virtual_Care_discussionpaper_v2EN.pdf
6. Webster P. Private telehealth foray into public system. CMAJ. 2016;188: E209–E209. doi:10.1503/cmaj.109-5285
7. Private virtual health services are booming in a 'policy vacuum.' In: thestar.com [Internet]. 17 Jan 2021 [cited 28 Jan 2021]. Available from: https://www.thestar.com/news/canada/2021/01/17/as-pandemic-rages-virtual-health-services-are-booming-in-a-policy-vacuum.html
8. Dialogue. Dialogue | Ultimate Guide to Telemedicine - for Canadian HR leaders. [cited 28 Jan 2021]. Available from: https://www.dialogue.co/en/ultimateguide-telemedicine
9. Infoway. The COVID-19 Experience: Canada Health Infoway Finds Canadians Trust and Have Come to Depend on Digital Health | Canada Health Infoway. 16 Nov 2020 [cited 28 Jan 2021]. Available from: https://www.infoway-inforoute.ca/en/what-we-do/news-events/newsroom/2020-news-releases/8856-the-covid-19-experience-canada-health-infoway-finds-canadians-trust-and-have-come-to-depend-on-digital-health
10. Glauser W. Virtual care is here to stay, but major challenges remain. CMAJ. 2020;192: E868–E869. doi:10.1503/cmaj.1095884
11. Shaw J, Jamieson T, Agarwal P, Griffin B, Wong I, Bhatia RS. Virtual care policy recommendations for patient-centred primary care: findings of a consensus policy dialogue using a nominal group technique. J Telemed Telecare. 2018;24: 608–615. doi:10.1177/1357633X17730444
12. Personal Health Information Protection Act (PHIPA), s 17(4).
13. Health Information Act (HIA), s 1(1)a.
14. Personal Health Information Protection Act (PHIPA), s 18(1).
15. Personal Information Protection and Electronic Documents Act (PIPEDA), s 6(1).
16. Glazier RH, Green ME, Wu FC, Frymire E, Kopp A, Kiran T. Shifts in office and virtual primary care during the early COVID-19 pandemic in Ontario, Canada. CMAJ. 2021;193: E200–E210. doi:10.1503/cmaj.202303
17. Lapointe-Shaw L, Salahub C, Bhatia RS, Desveaux L, Glazier RH, Hedden L, et al. Characteristics and healthcare use of patients attending virtual walk-in clinics: a cross-sectional analysis. medRxiv; 2022. p. 2022.02.28.22271640. doi:10.1101/2022.02.28.22271640
18. Hardcastle L, Ogbogu U. Virtual care: Enhancing access or harming care? Healthc Manage Forum. 2020;33: 288–292. doi:10.1177/0840470420938818
19. Toolkit WE. Virtual Health Care for Islanders without a Primary Care Provider. 23 Mar 2022 [cited 31 Mar 2022]. Available from: https://www.princeedwardisland.ca/en/service/virtual-health-care-for-islanders-without-a-primary-care-provider
20. CMA, CFPC, RCPSC. Virtual Care: Recommendations for scaling up virtual medical services. Report of the Virtual Care task force. 2020. Available from: https://www.cma.ca/sites/default/files/pdf/virtual-care/ReportoftheVirtualCareTaskForce.pdf
21. Marks M. Emergent Medical Data: Health Information Inferred by Artificial Intelligence. Rochester, NY: Social Science Research Network; 2020 Mar. Report No.: ID 3554118. Available from: https://papers.ssrn.com/abstract=3554118
22. Christl W, Spiekermann S. Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Facultas; 2016. Available from: http://crackedlabs.org/en/networksofcontrol
23. Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Back on the Data Trail: The Evolution of Canada's Data Broker Industry. 2018. Available from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2017-2018/p_201718_04/
24. CIHI. Best Practice Guidelines for Managing the Disclosure of De-Identified Health Information. Canadian Institute for Health Information (CIHI); 2010. Available from: http://www.ehealthinformation.ca/wp-content/uploads/2014/08/2011-Best-Practice-Guidelines-for-Managing-the-Disclosure-of-De-Identificatied-Health-Info.pdf
25. Information and Privacy Commissioner of Ontario, CHEO Research Institute. Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy. 2011. Available from: https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf
26. Privacy Analytics. IMS Health: Unlocking the Value of EMR Data for Advanced Research and Analysis, Better Health Metrics, and Product Innovation. QuintilesIMS; 2017. Available from: https://web.archive.org/web/20210216165758/https://privacy-analytics.com/wp-content/uploads/dlm_uploads/2020/06/IMS-Brogan-Case-Study.pdf
27. Rocher L, Hendrickx JM, Montjoye Y-A de. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun. 2019;10: 1–9. doi:10.1038/s41467-019-10933-3

28. Benjamin R. Assessing risk, automating racism. Science. 2019;366: 421–422. doi:10.1126/science.aaz3873
29. Regan PM, Jesse J. Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking. Ethics Inf Technol. 2019;21: 167–179. doi:10.1007/s10676-018-9492-2
30. Stockdale J, Cassell J, Ford E. "Giving something back": A systematic review and ethical enquiry into public views on the use of patient data for research in the United Kingdom and the Republic of Ireland. Wellcome Open Res. 2019;3. doi:10.12688/wellcomeopenres.13531.2
31. Aitken M, de St. Jorre J, Pagliari C, Jepson R, Cunningham-Burley S. Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. BMC Medical Ethics. 2016;17: 73. doi:10.1186/s12910-016-0153-x
32. Kalkman S, Delden J van, Banerjee A, Tyl B, Mostert M, Thiel G van. Patients' and public views and attitudes towards the sharing of health data for research: a narrative review of the empirical evidence. Journal of Medical Ethics. 2019 [cited 4 Dec 2020]. doi:10.1136/medethics-2019-105651
33. Paprica PA, de Melo MN, Schull MJ. Social licence and the general public's attitudes toward research based on linked administrative health data: a qualitative study. CMAJ Open. 2019;7: E40–E46. doi:10.9778/cmajo.20180099

SECTION 2: RESEARCH METHODS

In this study, we analyzed interviews and publicly available documents to gain insight into the privacy implications related to the commercial virtual care industry in Canada. We used a framework by Regan and Jesse to define the privacy-related ethical concerns that may arise when data are collected and used by commercial VCPs[1]. These areas of ethical concern include informational privacy, anonymity, surveillance, autonomy, non-discrimination and ownership of information.

IDENTIFICATION OF VIRTUAL CARE PLATFORMS OPERATING IN CANADA

From June 2021 to February 2022, we conducted structured internet searches to identify commercial VCPs operating in Canada. We defined a commercial VCP as a proprietary platform owned by a for-profit company that offers virtual care (telemedicine) services directly to patients. We included platforms that enabled remote communication between physicians and/or nurse practitioners and their patients. We excluded platforms that only provided remote monitoring or other services that did not involve a nurse practitioner or physician. We also excluded platforms that only provided enterprise virtual care (virtual care services exclusive to employees of an organization) and clinician-initiated virtual care platforms, as these typically do not have a publicly accessible website. We verified our findings with a recent environmental scan of commercial virtual care platforms in Canada[2].

IDENTIFICATION OF DOCUMENTS

For each commercial VCP we included, we identified the VCP company website, as well as relevant publicly available privacy policies and terms of service documents. To collect information on each commercial VCP, we also searched Mergent Intellect, a publicly accessible, web-based application offering business data for a collection of US and Canadian private and public corporations[3]. This database contains basic company information, as well as financial, industry, and executive details for over 1.6 million Canadian businesses. It offers information on corporate structures, including a list of key executives and a complete company family tree. We also used the Builtwith Technology Lookup online tool[4] to generate a technology profile for the identified commercial VCPs. Builtwith provides users with company and technology profiles for business entities of interest and identifies the software services, including analytics and tracking, eCommerce, advertising, webhosting, and content delivery network services. Using this tool, we were able to identify the different analytics and tracking software services integrated within the websites of the commercial VCPs.

INTERVIEWS

We identified potential interviewees through online searches of commercial VCPs and affiliated parties, LinkedIn, and through professional connections. Interviews gave participants the opportunity to discuss and reflect on their experiences and to share opinions of working within the commercial virtual care industry in Canada. To protect participant anonymity, all identifying information was removed from the transcripts prior to analysis. Participants are identified by pseudonyms in this report.

ANALYSIS

We extracted data from each commercial VCP's primary website and the Mergent Intellect database to provide a description of the commercial VCPs operating in Canada. We used thematic analysis to analyze the interviews and company documents[5]. We included all interview transcripts but used a sampling frame to select documents that were most likely to provide rich information on privacy practices of the range of companies operating in Canada. Data collection and analysis occurred simultaneously. We began by familiarizing ourselves with the data. For each document and interview, we created a memo summarizing the text, offering interpretation, and identifying lines of inquiry. We conducted preliminary coding, and as the analyses progressed, we identified themes, which we continuously re-evaluated as more data were collected and analyzed. Throughout the collection and analysis, memos were used to record thought processes, decisions, and uncertainties[6]. We also used a constant comparative method where new data were compared to the analyzed data, which further directed data collection for documents and interviews[6]. As part of the analysis, we assessed for privacy related risks and ethical concerns. At the same time, we sought to understand how individuals, diverse groups, and the Canadian society might be affected by these risks and potential harms.

LEGAL ANALYSIS

The legal team conducted primary legal research by reviewing the federal and provincial privacy legislation relating to PHI, with a primary focus on Alberta and Ontario, as examples of provincial health information acts. We also looked to any other secondary sources that indicated how commercial VCPs are governed by privacy legislation in Canada, and conducted comparative research in other jurisdictions, for example the European Union, that provided examples of more robust privacy protections. We consulted the provincial and federal laws on their respective websites[7–9]. Our secondary research included identifying relevant articles, bulletins, and interpretations of the various privacy legislations as they relate to commercial VCPs. Additionally, we consulted officers in the Ontario and Alberta OIPC, as well as the OPC via informal telephone interviews. We sought to understand the complicated legal landscape of interacting public and private sector privacy laws on this emerging and expanding area of health care using commercial platforms, both to describe the existing laws and to answer and research any questions that came up during the qualitative research.

References

1. Regan PM, Jesse J. Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking. Ethics Inf Technol. 2019;21: 167–179. doi:10.1007/s10676-018-9492-2
2. Matthewman S, Spencer S, Lavergne MR, McCracken RK, Hedden L. An Environmental Scan of Virtual "Walk-In" Clinics in Canada: Comparative Study. J Med Internet Res. 2021;23: e27259. doi:10.2196/27259
3. Mergent Intellect. In: Toronto Public Library [Internet]. [cited 17 Jan 2022]. Available from: https://www.torontopubliclibrary.ca/detail.jsp?Entt=RDMEDB0188&R=EDB0188
4. BuiltWith. In: BuiltWith [Internet]. [cited 30 Mar 2022]. Available from: https://builtwith.com/
5. Green J, Thorogood N. Qualitative Methods for Health Research. 3 edition. Los Angeles: Sage Publications; 2013.
6. Fram SM. The Constant Comparative Analysis Method Outside of Grounded Theory. The Qualitative Report; Fort Lauderdale. 2013;18: 1–25. doi:10.46743/2160-3715/2013.1569
7. Alberta Queen's Printer. [cited 27 Mar 2022]. Available from: https://www.alberta.ca/alberta-queens-printer.aspx
8. e-Laws. In: Ontario.ca [Internet]. 24 Jul 2014 [cited 27 Mar 2022]. Available from: https://www.ontario.ca/laws
9. Branch LS. Consolidated federal laws of Canada. 31 Jul 2015 [cited 27 Mar 2022]. Available from: https://laws-lois.justice.gc.ca/eng/

SECTION 3: OVERVIEW OF PLATFORMS OPERATING IN CANADA

We identified 61 commercial VCPs, owned by 54 companies, operating in Canada (Table 1). Most of the VCP companies were privately held (49/54, 91%) and based in Canada (51/54, 94%). Of the 61 platforms, six operated in provinces that did not fund direct-to-patient virtual care. In total, 14 (25%) of the VCP companies had relationships with chains of pharmacies — either through partnerships or as a subsidiary. The majority of platforms were a website-only service (39/61, 64%), while seven (11%) were only a mobile app and 15 (25%) offered both platform types. Most of the platforms offered primary care services (46/61, 75%) and 15 (25%) provided only specialized services such as pediatric, psychiatric, dermatology, and HIV prevention. Almost all the platforms (57/61, 93%) employed at least one analytics and tracking software service on their website.

Table 1: Overview of commercial virtual care platforms (VCPs) with direct-to-patient services operating in Canada

		No. (%)
Headquarters	Canada	57 (94%)
	US	3 (5%)
	Other	1 (2%)
Ownership	Publicly traded	8 (14%)
	Privately held	53 (87%)
Launch Date	Launched in Canada before March 1st 2020	27 (45%)
	Launched in Canada after March 1st 2020	13 (21%)
	Not specified	21 (34%)
Regions of Operation	All provinces and territories	12 (19%)
	Select provinces and territories	37 (61%)
	Not specified	12 (19%)
Payment	Operate in provinces with funded direct-to-patient virtual care	25 (40%)
	Operate in provinces without funded direct-to-patient virtual care	6 (10%)
	Operate in both systems	15 (25%)
	Unclear	16 (25%)
Types of Services	Primary care/general care	46 (76%)
	Pediatrics only	2 (3%)
	Dermatology only	2 (3%)
	Psychiatry only	1 (2%)
	HIV prevention only	4 (6%)
	Men's health only	6 (10%)
Platform Type	Mobile app only	7 (11%)
	Website only	39 (64%)
	Both	15 (25%)
Modalities	Video	39 (63%)
	Audio (e.g., phone calls)	33 (54%)
	Text/chat/messaging	16 (26%)
	Not specified	9 (15%)
Relationships with Pharmacies	Partnered with chains of pharmacies	6 (10%)
	Parent corporation/company also owns pharmacies	8 (13%)
Analytics/Tracking Software on Website	Used at least one service	57 (93%)
	No evidence of use of any services	4 (7%)

US = United States

KEY INFORMANTS AND DOCUMENTS

We interviewed 18 key informants affiliated with 12 different companies with commercial VCPs between October 2021 and January 2022. Nine participants were employees of companies with VCPs and 9 were individuals who had affiliations with the industry as consultants, academic researchers, or third-party subcontractors. Lettered pseudonyms were assigned to participants as to not identify them (Table 2). We also collected 30 documents from the 54 VCP companies and used a sampling frame (see Methods) to select 10 of these for analysis (Table 3).

Table 2: Descriptions of study participants (key informants)[1]

Pseudonym	Primary Affiliation	Role(s)
AM	Small health IT company with a VCP	CEO
FR	Small VCP	Employee
HT	Small VCP	Director
QC	Small VCP	Privacy Officer
JV	Large VCP	Data Analyst
PB	Large VCP	VP
LX	Large VCP	Director
MY	Large company with a VCP	VP
IU	Large company with a VCP	Physician
NZ	Multinational technology company	Cloud Engineer
OA	Multinational technology company	Security and Privacy Specialist
GS	Multinational consulting company	Digital Health Consulting Manager
RD	Multinational consulting company	Digital Health Consultant
KW	Multinational technology consulting company	CEO
BN	Technology consulting company	Executive Director
DP	Digital health privacy and security consulting company	CEO
EQ	Academic hospital	Physician and researcher
CO	Academic hospital	Physician and researcher

VCP = Virtual Care Platform; US = United States

[1] All initials are pseudonyms. They are not the participant's initials.

Table 3: Descriptions of documents analyzed

Pseudonym	Company Description	Company Headquarters	Policy Description
Company A	Small Canadian VCP	Canada	Privacy policy & terms of use
Company B	Large Canadian company with a VCP	Canada	Privacy policy
			Cookies policy
Company C	Small Canadian company with a VCP	Canada	Privacy policy
Company D	Large multinational company with a VCP	US	Canadian privacy policy
			Canadian virtual care privacy policy
Company E	Small Canadian VCP	Canada	Privacy policy
Company F	Small Canadian VCP	Canada	Privacy policy
Company G	Large Canadian VCP	Canada	Privacy policy
Company H	Large Canadian company with multiple VCPs	Canada	Privacy policy

VCP = Virtual Care Platform; US = United States

SECTION 4: THEMATIC ANALYSIS

4.1 SOLVING PROBLEMS AND HERE TO STAY

SUMMARY

Study participants viewed commercial virtual care as solving problems in the Canadian healthcare system by improving access to care and diverting visits from the overwhelmed emergency department. Participants also discussed how commercial VCPs were able to provide discreet care and specific expertise. Participants believed commercial virtual care was "here to stay" and promoted the narrative that the public sector was unable to create efficient and innovative solutions. They called for some adjustments to the commercial virtual care model, increased public funding for commercial virtual care and enhanced regulation that constrains problematic data uses, but allows for innovation.

ADDRESSING GAPS IN CARE

Participants believed that commercial VCPs were improving care for individuals by addressing gaps in the "over-taxed" Canadian health systems (DP[1], CEO at a digital health privacy and security consulting company). Participants described how they saw the platforms providing rapid and convenient access to care, something beyond what they believed was available in the current health systems. A physician and researcher at an academic hospital explained,

> **I think we really have to understand that access and convenience is important. And patients care about it. And we can't just keep saying to them, oh, you know, continuity wins above all, even if you have to wait to see the person for three days. That's sort of been our messaging and our stance, the way we operate, but it's not true and we're seeing that with patients using these systems. So, I think they fulfil a need in the system.** (EQ)

This statement suggests that commercial virtual care is fulfilling a need that has been downplayed by those with power, such as physicians, in the current health system. Participants also discussed how commercial VCPs could create an accessible healthcare service for underserved populations. An employee at a small commercial VCP, FR, described how commercial virtual care can improve access to care for groups who are stigmatized and face discrimination when they interact with the health system. Commercial VCPs provide these patients with access to providers with appropriate expertise in a "discreet welcoming" (FR) environment. By emphasizing rapid access over continuity of care, these statements also suggest that all patients within the Canadian health system are 'underserved,' and are marketed an alternative — commercial VCPs — where patients could rapidly access primary care on their own time.

[1] All initials are pseudonyms. They are not the participant's initials.

DIVERTING PATIENTS FROM THE EMERGENCY DEPARTMENT

Participants also believed that the use of commercial VCPs diverted visits from the emergency department. The VP at a large company with a VCP described further,

> **For the health care system, through our access, we could be, and are likely reducing costs on the healthcare system. For instance, if somebody is needing a telemedicine offering commercially, they may be able to get their issue resolved immediately, which they would have likely before had to go to the Emergency Room. That Emergency Room, whether it be volume of people, or cost was avoided because that person was able to get access commercially.** (MY)

Another participant, a Director at a large commercial VCP, described how the company she works for helped the provincial government divert emergency department visits.

> **A lot of individuals, either through their remote regions or just a lack of GPs [General Practitioners] in [Province X], they're not able to get the primary healthcare that they needed. So, the example was, like going to the ER for a prescription refill, which puts undue pressure on our emergency rooms. So, after having a few years as a company, we worked with [Province X] to [provide virtual care], I think the program was called [Virtual Care Program X].** (LX)

These statements imply that the current primary care systems are stretched, meaning that patients can only access timely care through emergency departments, which may not be an appropriate or cost-effective level of care. Participants, therefore, positioned the commercial VCPs as a means of relieving pressure on the system by providing timely access to primary care. The description of the partnership with a province may be seen as giving further weight to this claim — even public payers believe that commercial VCPs reduce the burden on emergency departments. These statements, therefore, promote the narrative that the commercial virtual care sector is a cost-effective solution to problems in the current health systems in Canada.

THE PUBLIC SECTOR CANNOT INNOVATE LIKE THE COMMERCIAL VIRTUAL CARE INDUSTRY

In the view of participants, the public sector was not able to create effective virtual care solutions. LX, a Director at a large commercial VCP, explained,

> **Because I think, this sounds really terrible, but a lot of the software engineering that we've seen throughout the pandemic, that has come directly from the public sector, particularly around healthcare, has been either, essentially, slow to the market, has been unstable, a little bit risky. And I think how the private sector is able to kind of move quickly and use best practices that are pulled from other areas of software development, we can really get stuff to market faster, get stuff to consumers faster, and work in partnership with regulation and the government, to kind of service need that we see really increasing.** (LX)

A Digital Health Consultant at a multinational consulting company explained why the public sector struggled, "they just didn't have the resources, or time, or motivation before pandemic to do it, and when they had the motivation, they didn't have the resources to build it" (RD). According to RD the public system lacked the motivation because it was not focused on patient needs.

> **We, in Canada, have been a very paternalistic healthcare system where if the doctor says something, you shut up and listen. We've gone away from that with these companies because they are consumer-focused companies who can make money only if you get a good experience, so the experience has gone up for people.** (RD)

Participants saw a shift in the rights and responsibilities of patients with the emergence of commercial VCPs. According to RD, patients before were passive and constrained recipients of care who needed to adhere to the physician's practices. With the rise of commercial virtual care, patients are re-defined as consumers of care who have choice and control over their care journey. As such, RD believes that commercial virtual care puts consumers wants and needs first, because as part of the private sector, companies need to please the consumers to make money. Thus, private, for-profit VCP companies are more motivated to meet the needs of patients than a public system that does not have to worry about consumer needs or wants. Viewing patients as autonomous individual consumers, however, gives patients the responsibility for the management of their care journey instead of being part of a larger system of care that supports the well-being of the population. This, therefore, diminishes the responsibility of the commercial VCPs to ensure well-being of the individual patient and the broader population.

Participants explained how the size of the companies creating and operating commercial VCPs gave them an advantage in terms of scaling virtual care services. A physician and researcher at an academic hospital described further, "[large VCPs] manage capacity well" whereas "a mom and pop clinic does not dial up when health needs increase, wait times just get longer" (CO). Further, GS, a Digital Health Consulting Manager at a multinational consulting agency, described the public sector as too risk adverse to create effective virtual care models, seeing this as a cause of "inaction." As a result, GS stated, "the private sector and technology are very [quickly] outpacing what the public sector is providing and that is in response to consumer demands."

Therefore, participants believed that commercial VCPs solved problems for the public system — "Because, again, health systems, you have to understand, are under a lot of pressure, so having somebody else figure this problem out for them, I think is the most important thing" (RD). Participants positioned this as a cost saver for the public system. A Privacy Officer at a small commercial VCP explained,

> **"It saves resources in the sense of human resources at a public level. It's not the government services that are having to come up with these innovative products. Technology is very costly, and it is costly to maintain. And so, by putting that back on the private companies, and then that allows for, in a market where there's an open market, competitiveness around being innovative and creating something that's really easy to use and that people will actively use. So, there's benefit there."** (QC)

She further stated, "I really genuinely see mostly benefits. Again, when it comes to the public system, I don't see it as an us versus them type of a situation. I think it's about making improvements to the overall system, and I think that there's an appetite to work collaboratively to achieve those means."

At face value, these statements suggest that the public sector is incapable of creating efficient models of virtual care, and therefore, needs to work with the private sector. The statements also promote the narrative that the government saves money by enabling the private sector to take on the burden of developing innovations. They imply that the private sector is uniquely positioned to do so because the competition feeds innovation and leads to the creation of effective solutions.

TWO-TIERED SYSTEM

Participants were concerned that commercial VCPs may create a two-tiered system in provinces where the governments did not fund direct-to-patient virtual care. In these provinces, only some employers or insurers funded access to commercial VCPs, while others had to pay out of pocket. According to GS, a Digital Health Consulting Manager at a multinational consulting company, this inequality in access was creating "the biggest threat to the universality of healthcare in real terms that's really existed in Canada since its advent." Participants, however, believed this challenge was easy to solve — all provinces needed to "start coming on board" (LX, a Director at a large VCP) and fund commercial virtual care. This statement implies the emergence of two-tiered healthcare is not due to the rise of commercial VCPs, but rather a failure of the provincial governments to fund the services. According to study participants, therefore, the problem of two-tiered healthcare is best addressed not by examining if commercial virtual care is the best solution, but by ensuring that public funders pay for the commercial virtual care services in every province and territory.

CONTINUITY OF CARE

Participants also expressed concerns that as the commercial VCPs were not "fully integrated into the rest of the system" (KW, a CEO at a multinational technology consulting company), they may disrupt the "continuity of care" because the patient data is "all over the place" (JV, a Data Analyst at a large company with a VCP) and creating "a highly fragmented system" (CO, a physician and researcher at an academic hospital). The VP of a large commercial VCP explained how fragmented care could harm a patient.

> **"If you strayed away from that, and you're just doing transactions — I've got the sniffles today, I broke my toe the other day — and the doctors don't talk to each other, or we don't provide a platform for at least a massive amount of information, then you're dealing with poor solutions, and you could miss things. That toe and that cough could be related to the same fungus, and it won't be found out because … and let's say in the commercial world you get one consult from Company X, and you get the second consult from Company Y, they don't know about each other, they don't know about what the other person had prescribed or said to each other. We don't have a central clearing house of records or drugs."** (PB)

This statement also reveals a different interpretation of continuity of care. Instead of defining continuity as care by the same provider over time, it is presented as the integration of data — "information sharing between these realms" (GS, a Digital Health Consulting Manager at a multinational consulting company) — so that multiple providers can have access to a patient's health records. This implies that fragmented care could be solved by better sharing of patient records, rather than a consistent primary care provider.

PROBLEMATIC DATA PRACTICES

Participants also raised concerns about what they saw as problematic approaches to collecting, using, and sharing data. These concerns are discussed in subsequent themes. To address these data practices, participants had a range of views, but generally described better regulation as the solution.

> **[Privacy legislation for commercial VCPs is] essential, of course. That's why we have health privacy laws. We have privacy laws relating to business information, private sector, public sector. It lays down the framework, the foundation of what is required. [...] Private sector privacy laws are not in existence everywhere. Ontario has not had one, but they're devising one now, private sector privacy legislation to complement the public sector and their health information privacy. All areas must be addressed.** (BN, Executive Director at a technology consulting company)

As CO, a physician and researcher at an academic hospital, expressed, "[commercial VCPs] build good IT backbones. So, you've got to leverage what's good about these companies and then constrain their behaviour in other ways, which I think hasn't been done adequately." However, some participants felt that regulators needed to be careful. As a Privacy Officer at a small VCP explained, while regulation can add more "clarity" and "guidance" for VCP practices, they must not be "restrictive to innovation" (QC). Thus, because of the important service commercial VCPs provide to patients and to the healthcare system, regulatory bodies should create a supportive climate to enable innovation and the development of new technologies. Participants thus promoted the view that commercial VCPs were an essential part of the healthcare system. They called for adjustments and careful regulation but did not question whether commercial VCPs were an appropriate model of care. Thus, participants believed that, with some adjustments to the model and enhanced regulation, commercial VCPs were legitimate— being in accordance with accepted rules and practices — and a viable part of Canadian health systems.

4.2 DATA DEFINITIONS AND DISCOURSES

SUMMARY

Participants described the different types of data that VCP companies collected and managed through the platforms, including user data and personal information. VCP companies generally separated the personal information into two categories, registration/sign-up data (i.e., names, email addresses, etc.) and PHI. This had implications for how data were treated by VCP companies. PHI was stored securely in an electronic medical record system, used only for clinical care, and de-identified before being used for any secondary reasons. Registration/sign-up data, user data and de-identified health information were part of the "business side" of the operations, and used for a variety of purposes. Participants, however, raised concerns about dichotomizing data this way and provided examples of how user data and registration information can reveal sensitive health-related information about individuals when used internally or shared with third parties. They also described risks (e.g., privacy loss, microtargeting, biased artificial intelligence (AI)) associated with the creation and use of de-identified data.

PHI AND PERSONAL INFORMATION

Participants described how commercial VCPs divided the personal information they collected into two categories. The first category was PHI — the data collected when patients interacted with health care providers, such as medical history, medications, family history and name of care provider. The second category was the data collected by the commercial VCP when individuals signed up or registered with the platform (e.g., name, email address, home address, IP address, device information) or submitted inquiries. According to participants, the commercial VCPs defined these data as personal information but not PHI category. VCP company documents aligned with these definitions. The privacy policy and terms of use from a small VCP provided this description of "personal information,"

> **"For the purposes of this Privacy Policy, "Personal Information" includes your name, phone number, email address, gender, birth date and internet protocol (IP) address used to connect your computer to the internet, but excludes Personal Health Information [PHI]; [...]** (Company A)"

The policy went on to describe how they defined PHI,

> **"Personal Health Information" means information that is collected or created by our healthcare team in the course of providing healthcare services to you, including information concerning your physical or mental health history, health status, symptoms, diagnosis, laboratory testing results and diagnostic images, information concerning any healthcare service and advice provided to you by us, including referrals, recommended follow up or next steps, and other health-related information.** (Company A)

The approach to exclude registration data and other personal data collected by the platform from the definition of PHI had implications for how the data were treated. The CEO of a multinational technology consulting company explained how the data they defined as PHI may be used,

> **[PHI is used] only to schedule the visit, to conduct the session, and it is being only collected and to be used for the primary purpose, which is to provide that patient with a virtual exchange with their physician. That is it.** (KW)

Thus, VCP companies only used PHI for the reason it was collected — to provide clinical care. This protects PHI by minimizing the number of people who have access to the data. Further, PHI was not shared with other entities except for essential functions like data storage or billing. The other data, for example sign-up information, as described in subsequent themes, were used for a variety of purposes. The privacy policy for a large company with a commercial VCP outlined how these data may be used,

> **Your name, email address, and home address may be shared within the [Company B] Family and matched to your existing [Company B] customer profile (if applicable) to identify other services that you have with the [Company B] Family. This information may be used to: Perform aggregated reporting and demographic analysis; Ask for your feedback on our Services through surveys or other means; and Help us and the [Company B] Family provide better recommendations of [Company B] products and services that may be of interest to you and exclude those that are not relevant.**

Together, these statements demonstrate that some platforms excluded the data collected when individuals registered to use the health service from the definition of PHI. These registration/sign-up data are on the "business side" (AM), implying they can be used for profit-making reasons.

CONCERNS AND COUNTERPOINTS

Some participants, however, expressed concerns about excluding registration/sign-up information and other identifying information from the definition of PHI. DP, a CEO at a digital health privacy and security consulting company, felt that VCP companies may be defining PHI too narrowly. He stated that the definition of PHI "is a lot more than people realize." In addition to medical conditions and medications, it also includes "things like what's my name and my address and my phone number" (DP). This statement implies that platforms cannot separate the registration information (e.g., an individual's name, postal code, and email) from where the data were collected, which in this case is a virtual care platform, and the purpose of collection, which is to request care. According to these participants, data are inherently PHI, because when the VCP company uses them internally for analysis, or provides them to a third party, the data are coming from a website or an app that provides a medical service. The data and commercial VCP are inextricably linked, therefore, revealing information related to an individual's health.

DE-IDENTIFIED PHI

Participants also described how VCP companies used the data they collected to create another form of data — de-identified health information. De-identified health information has identifiers like name and date of birth removed, and other quasi-identifiers, like postal code, modified until the probability of re-identification is low. According to participants, de-identifying PHI enabled companies to use the data for reasons other than providing clinical care because they no longer defined the data as PHI. Accordingly, the Canadian privacy policy for a large multinational VCP company stated they have the "unrestricted title, rights, and interest to it which may include, without limitation, the right to use, disclose, rent, or sell the de-identified information" (Company E). Hence, the data no longer belongs to patients, but are re-defined as an asset a company can use without restrictions.

Participants had a range of views on whether this unrestricted use of de-identified data posed risks to patients. The Executive Director at a technology consulting company stated, "If the data are strongly de-identified, you can virtually eliminate the privacy risks" (BN). When asked if there were any concerns about PHI data being re-identified or used for other reasons, a VP of a large commercial VCP stated,

> **"There's no concerns because you'll never reach an individual's data. [...] None. Again, we cannot have individual data of any kind leaching out of our system. Everything that is going to be tracked, anyway."** (PB)

These statements suggest that de-identification, when done properly, eliminates the risk of re-identification. It also implies that re-identification is the only risk associated with secondary uses of PHI and once eliminated, these other uses carry little to no risk to patients.

Some participants, however, expressed that de-identified data were not risk-free given that datasets are frequently linked (connected) with other datasets, increasing the risk of re-identification of individuals. As a Digital Health Consulting Manager at a multinational consulting agency explained,

> **Because what might seem de-identified in one dataset can be quickly identified when you start to add your insurance information or add your genetic information. I think that there is a potential risk there... I guess there is the potential there, where certainly the private sector is going to be more apt to look at those partnerships and how they combine and share data.** (GS)

Furthermore, "what is truly de-identified can depend a bit on the source and the details of the data included" (EQ, a physician and researcher at an academic hospital). De-identification is not a simple task. Determining the risk of re-identification depends on the nature and amount of information, which changes as soon as more data are added in, for example by linking datasets. Hence, the risk of re-identification remains unpredictable. Participants also pointed to other risks from de-identified data. EQ shared how aggregate data, created by combining multiple patient records into one record, can cause harm,

> **Even with aggregate data. If certain types of people or groups of people become stigmatized based on the aggregate data. You know, sort of saying, everyone from X group has X disease, because they don't exercise and it's their fault. That kind of stuff can happen out of the de-identified data, if it doesn't have proper oversight and participation. So, that's a risk.**

EQ later noted that legislative oversight on "where the data is going and what it is being used for" is important, and "ideally there's a line that says you can't monetize the data in any form" and that patients have "control over how their data is used." Through clearer legislation, patients can "make an informed decision" around their comfort level with commercial VCPs' collection and use of their data. This statement reveals how using aggregated de-identified data can (re)produce social stigmas surrounding particular populations or health conditions, and the importance of legislation in mitigating this risk.

USER DATA

Commercial VCPs also collect information using cookies and other trackers as individuals browse the internet and access commercial VCPs via an app or website. The platforms privacy policies and participants often referred to these data as user data and consumer data. The privacy policy of a small Canadian company with a VCP describes these data,

> **Specific types of usage information that may be collected automatically include: information about how, when and where you use our website; the hardware and software you use to interact with our website; your device identifier; your mobile network information; the settings you use on our website; your network location; your IP address; and information about the webpages you visited prior to coming to our website.** (Company C)

Therefore, these data contain identifiers despite not containing the names of individuals and being defined by the company as "non-personal" information — "we have no idea who is who" (FR, employee at a small VCP). Participants explained data brokers, like Google and Facebook use these identifiers (e.g., IP address) in the data to link the information to a uniquely-identified user in their database.

> **So, if anyone ever comes to our website just like a message gets sent back to Google that this person with this random identifier came to our website and then that just goes into the machine. Google does Google stuff with it.** (FR)

FR explained that many companies — "like 95% of the websites in the world" — share data with a data broker company for analytics to understand website users. He went on to state, "Just by doing that you are giving all of the information back to Google and then they are reselling that in the form of ads to other people." He explained further,

> **Google just knows if you have these specific things, like maybe you're more interested in your health or [in X health condition] you might be more interested in our service. They just sort of figured that out without us even knowing how it works. Both amazing and scary [...] So like in our case if you know that since someone went to [website X] that they might be more likely to click on [our advertisement]. That's how it's being sold. It's not sort of as clear and as easy to understand to a lot of people, but it's sold. [...] And they'll actually experiment with sending different people or with different interests and with different demographic information and it's very, very accurate. It's kind of amazing they know so much about you.** (FR)

Thus, third-party data brokers can link user information collected by commercial VCPs to a uniquely identified person to create a detailed profile containing information relating to an individual's health. Advertisers then bid, using pre-specified conditions, to advertise to these individuals, based on their profile and internet searches. As such, patient's user data, containing identifiers like IP address, but no names of individuals, are being given to third-parties, who are linking it to a uniquely identifiable profile (even if not by name) for the purpose of enabling targeted advertising. This may be particularly problematic if a platform only provides one type of health service, for example, is "focused on mental health," revealing the specific nature of the patient's health concern (OA, Security and Privacy specialist at a multinational technology company).

In some cases, VCP companies linked the user data to registration information. The privacy policy from a large multinational company, Company D, with a VCP states,

> **"Because certain transactions and activities are available to you on the Platforms, [Company D] must be able to link your activity back to your identity, so that changes in our systems can be made and we can track the Services you used. As such, the following information will be collected and identifiable to you:**
>
> - **IP address (the computer's address on the Internet)**
> - **Operating system (e.g., Windows 10)**
> - **Browser software (e.g., Internet Explorer, Chrome)**
> - **Internet Service Provider (e.g., Bell Canada)**
> - **General Geographic location (e.g., Toronto, Canada)**
> - **Type of device (e.g., iPad, desktop)**
> - **Mobile device crash information**
> - **Locale and language of device and whether it has fingerprint/face sensors**
> - **Dates and time you accessed and used the Platforms, features you used in the Platforms, and how long you use the Platforms overall**
> - **Links you click and pages you view within the Platform Pages you view before and after you leave the Platform"**

These statements demonstrate that data brokers (and some companies with commercial VCPs) are able to link the data to a uniquely identified user and track that person across the internet. Data brokers and commercial VCPs can use the information to build a sophisticated profile of that individual that may include health-related information, which can have value for advertising or other commercial purposes.

4.3 DATA ARE THE NAME OF THE GAME

SUMMARY

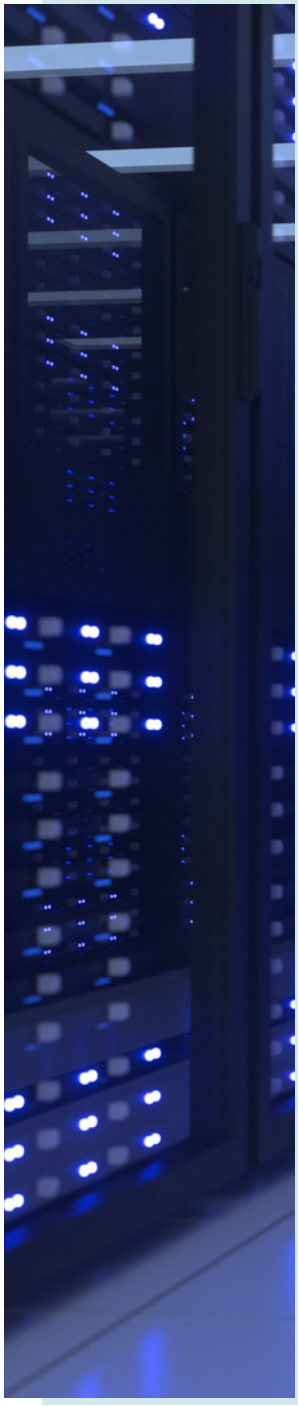
Participants described a massive expansion in the commercial virtual care industry in Canada since the onset of the pandemic. Large corporations that did not have a commercial VCP created one or purchased companies with one. These large corporations entered the market, according to participants, because of an interest in health-related data. Participants described these data as valuable because they allow VCP companies to gain insight into the healthcare industry, create health system innovations and improve services. Data obtained from commercial VCPs also had value because they enabled VCP companies to effectively promote their products and services, as well as those of their business partners. Participants also described situations where VCP companies used data to influence the patient's health care journey with the goal of increasing uptake of a product or service.

DATA ARE THE NAME OF THE GAME

The pandemic brought about a major expansion in the commercial virtual care market in Canada. As stated by a physician working for a large company with a VCP, "During the pandemic, if it says Telemedicine on it, you're getting investors and you're getting bought up" (IU). In participants' experiences, access to health/health-related data, was one of the primary reasons companies were entering the market. The CEO of a small health IT company with a virtual care platform stated, "That's kind of the name of the game, to be honest" (AM, a CEO at a small health IT company with a VCP). Likewise, the CEO of a digital health privacy and security company characterized the industry expansion in the area as a "gold rush" driven by data.

> **Part of what we see here is a little bit of the software gold rush into healthcare that says the future is data and look at all the things we can do when we aggregate all of this data together to come up with insights. And those insights are competitive advantages that can then be monetized.** (DP)

For this participant, "competitive advantages" can arise from companies having "the ability [...] to see things in the future based on trends from the past," which allows for companies to plan business strategies and develop technologies accordingly, so that their platform is more attractive than others. Data, therefore, are a highly coveted "asset" (LX, a Director at a large VCP) not just a side product or a digital exhaust, but one of the major drivers of expansion in the virtual care market, which accelerated during the pandemic through rapid mergers and acquisitions.



VCP COMPANIES HAVE DIFFERENT DATA BUSINESS MODELS

Participants explained that not all VCP companies were using health data to the same degree or in the same way. Most VCP companies were collecting, analyzing, and sharing user data (e.g., IP addresses). Similarly, most VCP companies analyzed sign-up/registration information (e.g., names, email addresses) for business purposes. Some were also sharing this information with other subsidiaries of the parent corporation or with business partners for analytics and product promotion or with third parties for targeted advertising. Participants also described how some VCP companies were using patient data to run advanced analytics and promote products for third parties without sharing any identified information externally.

However, participants believed all VCP companies wanted to use data for more advanced analytics once they had capacity to do so. As DP, the CEO at digital health privacy and security consulting company, stated, "To be fair, a lot of virtual care digital health platforms, that's their intention, but they don't even have enough data yet to make any large conclusions." A physician and researcher at an academic hospital explained that the size of the data holdings determined whether a data set could be used for more complex analyses, "A data set of 1,000 patients is not that valuable. A data set of 10,000, 50,000 patients becomes highly valuable" (EQ). Another participant agreed, "I think that when you see entities, as we have in Canada over the last year, go up for initial public offering and be valued at hundreds of millions of dollars, that part of that evaluation is also around the data that they have access to" (GS, a digital health consulting manager at a multinational consulting company). Larger data sets are more valuable because they permit more robust and accurate analyses. They provide a more accurate picture of the patient population and produce findings generalizable to the broader Canadian population. Hence, the ability to use data depends in part on the size and maturity of the company as larger VCPs with more patients and sophisticated data analysis technologies are more likely to use data for advanced purposes, like creating AI. Mergers and acquisitions where smaller VCP companies were acquired by large corporations are not just driven by need to grow, but also by the need to get enough health data to make monetizing it possible.

INNOVATIVE AND IMPROVE SERVICES

Participants described why the health data were valued by VCP companies. The data allowed VCP companies to monitor platform users' behaviours to improve their services and create new innovations. A VP of a large corporation with a VCP provided an example,

> **"[...] if we see that there's a particular condition that's a big need through virtual care, then we need to actually build a product that is specific to the offering and making sure that we're really meeting the need of that particular condition."** (MY)

For this participant, data are used to detect areas in care where there is "consumer" demand, but no (or inadequate) services to fulfill this gap. This helps the commercial VCP build or improve services to more fully meet the needs of patients. Likewise, creating and improving services expands and generates new markets, which meets the company's need of increasing profit. While this may seem like a win-win situation (i.e., both VCP companies and patients benefit from data uses), VCP companies may construct and advertise needs to patients that may not be necessary or helpful in order to create another stream of revenue.

PROMOTE PRODUCTS AND SERVICES

VCP companies also used data collected through their commercial VCPs to promote their other products and services, often ones that an individual "might normally paid out of pocket, like seeing a psychotherapist" (PB, a VP at a large VCP). KW, a CEO at a multinational technology consulting company, described how commercial VCPs used the personal information and user data to create a "profile of that patient" to market other services. A Director at a large VCP explained how this would be done,

> **Other ways that we would be using this information, that are kind of secondary and not immediate, would be to recommend additional services. As a private company, we need to make money, so we would be using additional services to recommend that for you, such as if you are frequently looking up dermatology terms on our app, we might offer additional services around dermatology for you. So, there is that kind of up-sell conversion idea that is in there.** (LX)

VCP companies use data to influence patient behaviours through suggesting products based on their activity on the VCP. These data uses are expected — and reasonable — as for-profit companies "need to make money" (LX) as well as "maximize shareholder value" (CO, a researcher and physician at an academic hospital). DP, a CEO at digital health privacy and security consulting company, described his view on monetizing data, "[commercial VCPs] can't be faulted for [using data for commercial purposes], that's a business and every business does it. So, I think that's interesting and not too terribly surprising."

Thus, VCP companies use patient data to inform their business practices and to market additional services to platform users. In this situation, it appears the amount the public system pays for virtual care services is not enough for VCP companies and shareholders who expect a certain amount of profit. The private sector, therefore, is subsidizing costs through data-driven business ventures, described by one participant (CO) as "money off [patients/users] backs." If VCP companies were no longer permitted to use data to support their business ventures (e.g., selling other products), the commercial model of virtual care may not be sustainable.

PROMOTE PRODUCTS AND SERVICES FOR THIRD PARTIES

VCP companies also valued data as they enabled profitable, data-driven business partnerships, often with pharmacies and pharmaceutical companies. These were not framed as selling data to a third party, but rather as sharing data or data insights with a business partner. AM, a CEO of a small health IT company with a VCP, described how it might work,

> **So essentially if we know a patient is coming through our website looking for men's health products, how do we direct that patient to seek a doctor for ED [erectile disfunction] meds [...] Or, if an individual is coming through our service looking for mental health resources, how do we lean them into some of our partnerships with corporate counselling services? So, that's kind of where that data is going to help individuals build these build these partnerships. And more often than not, they're with other corporate entities.**

Thus, VCP companies are looking for opportunities to match the services and products of their business partners to an appropriate patient. Some privacy policies indicated that commercial VCPs provided identified information (e.g., names, email addresses) to a third party for these promotional reasons. For example, the privacy policy for a small VCP company stated that the company may disclose personal information to "enable advertisers to provide you with more personalized content and track the effectiveness of certain advertising campaigns" and to "meet legitimate business and legal objectives" (Company F). Other policies clearly stated that the commercial VCP did not share personal information with third parties.

Participants provided examples of how commercial VCPs might use data to promote products for third parties without sharing identified information. In an example provided by a Director at a small VCP, his company partnered with a pharmaceutical company to send reminders to patients to increase use of the company's pharmaceutical product. He noted that the pharmaceutical company did not want individual patient data — "They were pretty upfront of not sharing patient sensitive data." Rather they wanted "anonymized data" on the success of the intervention.

> **What they were interested in was how successful the engagement was from the clinic's perspective and how educated the patient was about [the health condition]. The data points that they were looking at when the campaign started, the patient clicked on the link. How many times did they click on the clink? Did they view the ad, assets, and education material around [the health condition]? Did they book a consultation with their family clinic? And did they get [the pharmaceutical treatment]? We do capture sex, if they're male or female, because those are interesting things for the stats. And if they're not interested in getting [the pharmaceutical treatment], what were the reasons? And those are important data points that we can share with the pharmaceutical company.** (HT)

In this case, the pharmaceutical company used de-identified data to better understand and improve patient outreach and treatment adherence with the goal of optimizing the promotion through the platform. Further, since only aggregate data or data insights were shared, HT believed there were no or minimal risks or harms to patients.

Sometime VCP companies would hire other companies to facilitate third party promotion through their commercial VCPs. According to OA, a privacy specialist at a multinational technology company, the facilitator company would review the commercial VCP's de-identified patient demographic data, and then match the information with appropriate advertisers. He described the demographic data that would be shared with advertisers.

> **"Demographic age, demographic even ethnicity as you can imagine, where is location based on the healthcare application, because again now there are even specialized healthcare applications that are being out there, like things that I've seen in my previous employer, which are applications that are focused on mental health, while other ones are focusing on another type of illness. And then that information is being shared.** (OA)"

OA explained that the advertiser would then determine if "given the demographic that are accessing, maybe this would be a good spot to showcase a certain medication or whatever the case is." Again, OA described this as a "win-win" for advertisers, platforms and patients, as VCP companies are not sharing any identified information with third parties.

Similarly, an employee at a small VCP, FR, described how his “pharmaceutical-paid” and "data-driven” company sought to increase the uptake of the pharmaceutical sponsor’s product. His company tried methods like “sending [patients] a text message or adding more clarity around what benefit they’ll get” and then ran analyses via “A/B testing” to determine what methods were most effective. He further explained how his company would “put out a new version of our software and give that to a percentage of our users” and see if that improved uptake of the pharmaceutical product.

These software experiments functioned as an intervention in the patient care journey, with implications for patient health. These analyses can “facilitate kind of rapid cycle improvements” according to a physician and researcher at an academic hospital (EQ). They may also have a large impact as they “have the ability to influence perhaps the patient’s decision making into healthcare choices, perhaps more than ideal” (EQ). HT explained, “Consumers just kind of ignore stuff on TV now. And pamphlets, they might not read that when they’re at the clinic. But when a clinic actively engages the patient about the healthcare issues, it might work.” Since these recommendations and reminders are coming from a trusted source, a platform used by physicians to provide health services, patients may be more likely to respond to the promotional messages. These partnerships, therefore, may be very attractive to third parties like pharmaceutical companies.

Yet, using data to promote products and services also raised concerns for participants as the practice has implications for the quality of care. The CEO of a digital health privacy and security consulting company stated, “I would like my care journey to be governed by what’s the best care for me, not who paid the most amount of money to get in front of me for my attention” (DP).

FR expressed similarly that platforms may not provide the “best recommendations for your actual life in sort of a positive way” but rather may be “totally abused” for commercial gain. Thus, if patients’ care pathways are being influenced by pharmaceutical companies to increase uptake of their products, health decisions could be influenced by business goals instead of clinical judgement. Furthermore, according to FR, patients were not informed that such testing and 'nudging’ occurred (“they are not aware”), raising key questions about validity of patient consent.

DATA ARE A PROPRIETARY ASSET

Data, therefore, were valuable, and as one participant explained, would only be shared with partners when it provided a business advantage.

> **Yeah, we wouldn't be sharing that information with a third party. One, that's wildly risky. For no good reason. And two, data is our asset in terms of a business. If we were to distribute that to anyone else, it would be a business risk to us. Like, that is our advantage.** (LX, Director at a large virtual care platform)

LX suggested that she and the company she works for view the data they collect as a proprietary asset, one that should only be shared for a competitive business advantage, generally with a commercial partner. As explained by a CEO of a small VCP, "there isn't very much profit for a corporate entity to build an association with a public entity" (AM). Participants had concerns about what this might mean for the health system. As described by a physician and researcher at an academic hospital,

> **If a private company holds it and doesn't share it with integrated delivery systems that are not connected to other parts of the health system so that people can work together to provide better care, you're losing value. On the one hand, they are compromising patient trust potentially and making money in ways that don't improve public welfare. And on the other hand, by not sharing with public health systems and other providers, then they are compromising public welfare.** (CO)

For CO, commercial control over patient data may impair the ability of the public health system to conduct research, innovate, and improve their delivery and provision of healthcare.

4.4 CONSENT IS PROBLEMATIC

SUMMARY

Participants described consent as an essential part of how VCP companies gained access to an individual's data. Yet, the participants and VCP company documents pointed to many barriers to meaningful consent. Participants described how patients may not carefully evaluate VCP company policies, as they may have incorrect assumptions about how their data will be handled based on their experience with in-person care. Specifically, they assume their data will only be used to provide clinical care. Patients also may not be in the right frame of mind to carefully read policies when they are looking for urgent medical attention. Further, according to participants, the privacy policies and terms of services often use inaccessible language and contain vague descriptions of data flows and uses. They explained that the vagueness may be deliberate to avoid having to update policies or because data flows are complicated and hard to describe. Additionally, many platform policies appear to require patients to agree to many commercial uses of their data that are unnecessary for the provision of healthcare prior to accessing a health service. These include new product and service development and creation of targeted advertisements.

ASSUMPTIONS ABOUT DATA COLLECTION AND USE

Participants expressed that patients may have assumptions about how their data are collected, used, and shared, and as a result, may not carefully evaluate privacy policies. A physician and researcher at an academic hospital described what these expectations are, "I think their expectation also is likely that people on a care team have access to that information... most people don't think this information is shared with any other party that's not part of their circle of care" (CO). A CEO of a small Health IT company with a VCP explained why,

> **"I think patients assume that's private. When they hear virtual care and they hear licensed physician in Ontario or licensed physician in your region, I think we make assumptions that it's private. They assume ultimately if they come to see a doctor in the clinic, they make that same assumption.** (AM)

The public holds certain expectations around the collection and use of their data resulting from in-person care at a clinic or hospital. Patients, therefore, may assume that commercial VCPs are handling their data in the same way. A Digital Health Consultant at a multinational consulting company provided an additional explanation,

> **"I think it's very interesting because when I used to work in the U.S., I used to work at [Consulting Company] in the U.S. before, and the general consensus around people that I found out was that there was a lot of mistrust in any sort of healthcare establishment, whether government or not, in the U.S. However, in Canada, it's been very different where people, for some reason, or not for some reason, for good reason as far as their experience have had very good experience in privacy and security and aren't as worried about it, it seems like, from my experience. I think the expectations are, compared to the U.S., pretty low, in Canada at least, because people just generally have more trust."** (RD)

For RD, trust in healthcare systems in Canada can reduce concerns about how commercial VCPs manage patient data. Patients trust that these commercial entities are working in their best interest because they see them as healthcare providers and are "assuming security and privacy is taking place" (DP, CEO at digital health privacy and security consulting company). This can lower users' motivation to read, question, or challenge virtual care companies as they assume that they are following the same practices as the rest of the Canadian healthcare system.

Participants explained, however, that despite assumptions that data were only used to provide clinical care, "that's not what happens" (JV, a Data Analyst at a large commercial VCP). A physician who worked at a large company with a VCP concurred,

> **"I think if you asked most patients, they would probably think that the only people that have access to the data are the clinical team. And it isn't that. So, I don't think most people would even consider that their data could be accessed by anyone involved in the development of the app or anyone outside of the clinical team."** (IU)

When describing the mismatch between expectations and reality, some participants felt that patients also had some responsibility. A Director at a small commercial VCP explained, "As long as [the privacy policy is] upfront and [users] know how that data is being used and it's clear, then I believe that it's up to the patient to understand that" (HT). Patients, therefore, are responsible for understanding privacy policies as long as VCP companies clearly and transparently lay out how data are collected and used. The mismatch between patient expectations and the reality of data flows in virtual companies was sometimes considered as a generational difference. HT reported, "It's usually the older generation that have more of a concern than the younger generation who are kind of used to that through social media platforms, right?" By framing the issue as dependent on users' comfort and experience with new business models that are data-driven, these statements again shift some responsibility to platforms users for the mismatch between expectations and reality of data uses.

FRAME OF MIND

Participants also pointed to users' frames of mind as a barrier to meaningful consent. When accessing the services, platform users may be focused on an urgent medical situation and not able to examine complicated privacy policies. A Digital Health Consulting Manager at a multinational consulting company noted,

> **At the point of care or point of contact most individuals are worried about their rash or their cough or their daughter's sickness and they're not really thinking about what happens with that information over the long term, how it's leveraged and what it could be used for.** (GS)

Patients accessing commercial VCPs are vulnerable. As their main concern is attending to their health or the health of a loved one, they may not have the ability to carefully evaluate complicated privacy policies. AM, CEO of a small Health IT company, explained that "patients trust the interfaces that they're seeking care for during a time of duress."

INACCESSIBLE LANGUAGE

Some participants reported that privacy policies and terms of service documents were confusing and difficult to understand. The language used in these policies is not accessible to users of commercial VCPs. Rather, the policies are written in "legalese" (QC, Privacy Officer at a small commercial VCP) — for someone who has a legal background in health information technologies. The technical language can also make it difficult to hold the user's attention, as QC noted, "[The policies are] so dry, it's such a boring subject, that it is easy to kind of glaze over these things, and then also difficult to understand them." Hence, the lack of plain language limits patient's ability to provide consent. It may also affect their willingness to read the policies in the first place. AM, CEO of a small Health IT company, shared, "nobody actually reads the terms and services. They just scroll through it, check it off and then proceed." JV, a Data Analyst at a VCP company, explained, "how many of [the users] read [the policies]? I doubt very many. I know I hardly ever read privacy terms and conditions and I work in the industry." Thus, participants working in the commercial virtual care industry acknowledge that the policies are not written in plain language and are rarely read by patients.

VAGUE DESCRIPTIONS OF DATA FLOWS AND USES

Compounding the inaccessibility of privacy policies, participants noted how descriptions of data uses and flows were often vague. EQ, a researcher and physician at an academic hospital explained the policies,

> **If you weed through the details of [commercial VCPs] terms of use, they say they'll use the data. Some of them say they will kind of sell it to another party, some of them say they'll use it to make their product better, some of them say they'll use it for like sort of research, and they'll give more details. So, I find, you know, there's not a lot of transparency. A lot of it is happening, but there's not a lot of transparency around what it actually is.**

AM, CEO of a small health IT company, shared how general terms cover many different uses,

> **A lot of times, they use boilerplate terms like, 'we would use your data to improve our product or to enhance your experience.' But what that really usually means is we're going to use your data to figure out ways to improve the client experience or consumer experience to improve our bottom line or to improve partnerships to basically increase our profit. It is happening, but there's not a lot of transparency around what it actually is.**

This vague language may be deliberate. QC, a Privacy Officer at a small commercial VCP, explained that her company was instructed by the legal team to keep terms of use and privacy policies "general" enough to avoid having to update them. The vagueness may also be the result of complicated and difficult to explain data flows.

> **If a company is structured in different entities, there might only be a handful of people that actually understand the interactions between these different entities. Hypothetically, let's say you had virtual care company A that the patient is interacting with, but virtual care Company A sits under the umbrella of Organization B that also has entity C, D and E. These entities might all have data sharing arrangements with virtual company A. And maybe these entities don't actually understand that each one of them have data sharing arrangements. The only individual that understands the full lens is the umbrella company. So, that is something that's usually what I mean is a black box. You really sometimes don't understand the interaction by all the players involved that's associated with that company and that's interacting with the patient.** (AM)

As a result, data flows may be obscured to users and lower-level employees, with only top-level management having insight into the full extent of data flows and uses. This may include physicians working at commercial VCPs, who are ultimately responsible for the PHI collected by platforms. IU, a physician at a large company with a VCP responded to the question "for users of commercial virtual care platforms, how might you describe the ways that their data are collected, managed and used?" by stating that she didn't "know anything about the backend how the data is collected." Similarly, she explained that she did not know how the platform she worked for was handling de-identified health information. Legislation and regulatory requirements also may influence data flows, further complicating them. According to AM, "powerhouse legal teams" help design the data flows, some of whom "find creative ways of working around legislation." Another participant, OA, a Privacy and Security Specialist at a multinational technology company, explained how a "strong and thoughtful law department" might counsel the company around grey areas in legislation concerning data uses.

> **So, let's just build it, let's just do it, and we don't have to worry about it right now. And once it comes time to demonstrate our compliance, we can simply argue that is outside of our scope. And those instances have happened, right, again because the regulation is a law, and this is why our organizations employ parts of the department that focus on this.** (OA)

Data flows may be complicated to maximize data uses, while remaining in accordance with a VCP company's interpretations of the privacy legislation. Some higher level management and legal teams at commercial VCPs may be willing to take calculated risks in the grey areas of what the law permits, perhaps further complicating data flows. Thus, data flows within a company end up being difficult to understand, essentially a "black box" (AM) to all, but top-level employees, such as "CEO or like head of legal or head of business development" (AM). Thus, VCP companies may not be designing privacy policies to clearly inform users about the nature of data collection and uses.

DIFFICULTY OPTING OUT OF COMMERCIAL DATA USES

Participants described how it was difficult for patients to opt-out of commercial data uses (i.e., data uses for commercial purposes that are not necessary for clinical care) when accessing the health services provided by the platforms. As described in previous themes, these data types include user data, personal information, and de-identified information. Commercial data uses include marketing, research, and analytics. In some cases, companies shared these data types with third parties for commercial reasons. EQ, a physician and researcher at an academic hospital, explained the consequences if a patient did not want to share their data,

> **I think part of the problem is, if you don't believe in that philosophy, you know, whatever the other thing they're doing is, then you don't have a choice, you still have to access that service. So, it's kind of the fact that, you are supporting this other thing that you may or may not agree with, simply through accessing a healthcare service. Which is, you know, probably not appropriate.**

This statement indicates that not only was it difficult to opt-out, but that some platforms may make many commercial uses of data a condition of using the platform for a health service. Accordingly, the platform privacy policies did not appear to give patients the ability to opt-out of most commercial uses of data including the development of new products and services, and the creation of targeted (tailored) advertising and promotion on platforms. Privacy policies did instruct patients on how to opt-out of receiving marketing messages. Thus, to avoid most commercial uses of their data uses, a patient's only option may be to stop using the health service. The Canadian privacy policy of a large multinational company informs patients that if they do not want Company D to collect their personal information for the purposes outlined in their policy, they "must stop using the websites." Similarly, the privacy policy for a large Canadian company with a VCP states, "If you do not want us to collect, use or disclose your Personal Information or Personal Health Information in the ways identified in this [privacy policy], you may choose not to use [Company B's] Services." Further, the document states that when patients accessed the website "you consent to our collection, use, disclosure, and storage of your Personal Information as described in this Privacy Commitment." With respect to user data, such as IP address, cookies, and geolocation information, VCP companies seemed to give patients more control over the uses and collection of their data by informing them how to disable cookies and other tracking technologies. However, policies revealed that by default, users were automatically opted into the collection of certain kinds of data. Additionally, policies warned platform users that if they refuse to accept cookies and trackers, some of the services may not function. It is very difficult, and sometimes impossible, for patients to avoid commercial uses of their data when accessing health services through the commercial VCPs. This raises the issue of whether it is appropriate to require patients to consent to commercial uses of their data to access a health service.

SECTION 5: LEGAL ANALYSIS

5.1 HOW PRIVACY LAWS AND HEALTH INFORMATION PRIVACY LAWS INTERACT IN CANADA?

A. BACKGROUND

The Personal Information Protection and Electronic Documents Act (PIPEDA) was enacted in 2000 and governs the collection, use, and disclosure of personal information that is collected, used, or disclosed in the course of commercial activity[1]. PIPEDA applies to various subsets of personal information, including PHI. Therefore, physicians and surgeons fall under PIPEDA when they engage in private practice, but hospitals are presumptively excluded from its application[2]. Although PIPEDA is a national statute that applies to all provinces, where the Governor in Council (GIC) is satisfied that provincial legislation is "substantially similar" to PIPEDA, the GIC has the power to exempt particular organizations, activities or classes of activities[3]. The intent of this provision is to provide provinces with autonomy in regulating privacy within their borders. However, PIPEDA does not lay out the criteria for determining whether provincial legislation is substantially similar. The OPC has defined "substantially similar" as "equal or superior to" PIPEDA, positioning the federal law as a threshold[4]. In the 2002 Annual Report from the OPC to Parliament, former Commissioner George Radwanski determined that to satisfy the threshold for substantial similarity, the provincial statute would minimally need to include the 10 fundamental principles of PIPEDA, including consent, access and correction rights, the reasonable person test, and provisions supporting effective oversight and redress[5]. Industry Canada has published similar criteria for the Ministry of Industry, noting that substantially similar provincial or territorial legislation will: incorporate the ten principles in Schedule 1 of PIPEDA; provide an effective oversight and redress mechanism with powers to investigate; and restrict the collection, use, and disclosure of personal information to purposes that are appropriate or legitimate[6].

Québec, British Columbia, and Alberta have private-sector privacy laws that have been deemed substantially similar to PIPEDA (respectively Québec's Act Respecting the Protection of Personal Information in the Private Sector[7], BC's Personal Information Protection Act[8], and Alberta's Personal Information Protection Act[9], (Alberta's PIPA)). The exemption orders granted to these provinces free their commercial organizations from Part I of PIPEDA in respect to the collection, use, and disclosure of personal information. This exemption includes the collection, use, and disclosure of PHI by organizations as it is a subset of personal information. Additionally, Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have received an exemption from PIPEDA for the provinces' respective health privacy laws, which exempt their health information custodians from complying with Part I of PIPEDA in respect to the collection, use, or disclosure of PHI. These Acts include, in Ontario, the Personal Health Information Protection Act (PHIPA)[10]; in New Brunswick the Personal Health Information Privacy and Access Act[11]; in Nova Scotia, the Personal Health Information Act[12]; and in Newfoundland and Labrador, the Personal Health Information Act[13].

Alberta's privacy legal landscape is unique. As previously stated, Alberta's general private sector privacy legislation has been declared substantially similar to PIPEDA, but its health information legislation, the Health Information Act (HIA), has not[14].

It is important to note that the exemption orders are based on the nature of the activities rather than the type of personal information. For example, HIA-designated custodians that are also private organizations under Alberta's PIPA must manage the information they collect, use, and disclose in accordance with the applicable law depending on the activities. Therefore, when they provide a health service (e.g., providing treatment and care to a patient), the HIA applies. When providing a service other than a health service (e.g., managing employee information), Alberta's PIPA applies[15]. Although it is beyond the scope of this paper, commercial VCP compliance with health privacy legislation is also dependent on where their customers (the health custodians) are located, which further complicates the privacy landscape.

B. WHAT DOES IT MEAN FOR COMMERCIAL VIRTUAL CARE PLATFORMS IN ONTARIO?

It is difficult to discern how federal and provincial privacy laws intersect in relation to commercial VCPs. As private sector commercial organizations, VCPs are subject to PIPEDA; however, commercial VCPs may also be subject to additional requirements under PHIPA and its regulations where they are acting as an agent of a health information custodian, provide certain electronic services, or are classified as a health information network provider (HINP or provider).

To the extent that commercial VCPs carry out the purposes of health information custodians, they act as their agents. Under Ontario's PHIPA, agents of health information custodians are defined as "a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes [...]"[16]. Health information custodians include, but are not limited to, "a health care practitioner or a person who operates a group practice of health care practitioners"[17]. Therefore, in Ontario, commercial VCPs are currently subject to both PIPEDA and Ontario's PHIPA depending on the activities performed. To the extent that commercial VCPs are carrying out the purpose of health information custodians, and thereby acting as their agents, they fall under PHIPA.

The health information custodian is responsible for PHI that is in the custody of the agent[18]. Hence, health information custodians must take steps that are reasonable to monitor the compliance of the commercial VCPs that are their agents. Notably, in section 17(2) of PHIPA, it is required that a health information custodian must take reasonable steps to ensure that the commercial VCP does not collect, use, disclose, retain, or dispose of PHI unless it:

> (i) is permitted by the custodian in accordance with subsection (1),
> (ii) is necessary for the purpose of carrying out his or her duties as agent of the custodian,
> (iii) is not contrary to this Act or another law, and
> (iv) complies with any conditions or restrictions that the custodian has imposed under subsection (1.1); and
> (b) the prescribed requirements, if any, are met[19].

The agent has the responsibility to comply with the conditions and restrictions that are imposed by the health information custodian and is also responsible for notifying the custodian at the first reasonable opportunity if the PHI is stolen or lost or if it is used or disclosed without authority[20].

Even if a commercial VCP is not classified as an agent of the health information custodian under PHIPA, they may still be subject to additional limitations that are prescribed in the regulations under PHIPA[21]. Under s. 10(4) of PHIPA, anyone "who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information" ("providers of electronic services") must comply with the prescribed requirements. Section 6(1) of the regulations under PHIPA requires that any VCP that is a provider of electronic services must meet the following requirements:

> 1. The person [or VCP] shall not use any [PHI] to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services.
> 2. The person [or VCP] shall not disclose any [PHI] to which it has access in the course of providing the services for the health information custodian.
> 3. The person [or VCP] shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person who is subject to this subsection[22].

In addition, the regulations prescribe that HINPs must meet certain requirements as well. HINPs are defined as "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose [PHI] to one another, whether or not the person is an agent of any of the custodians"[23]. In the course of providing services that enable a health information custodian to collect, use, disclose, retain, or dispose of PHI, s. 6(3) of the regulations require HINPs to satisfy a series of requirements, including notice to custodians in cases of unauthorized access, providing plain language descriptions of services provided to custodians, and security and privacy assessments for the service provided; in addition, the provider is required to ensure any third parties they engage also comply with the regulations. Finally:

7. The provider shall enter into a written agreement with each health information custodian concerning the services provided to the custodian that,
i. describes the services that the provider is required to provide for the custodian,
ii. describes the administrative, technical and physical safeguards relating to the confidentiality and security of the information, and
iii. requires the provider to comply with the Act and the regulations[24].

Therefore, if a commercial VCP's relationship with a health information custodian meets the definition of a HINP, the restrictions and limitations in the regulations as described above may apply. As a result, a commercial VCP will be subject to additional obligations. There is a risk that health information custodians, in establishing these agreements, may not fully understand their obligations, or those of the VCP with whom they are contracting. However, depending on the sophistication of the parties and their relative bargaining positions, health information custodians may be able to impose contractual obligations on commerical VCPs — whether they are agents, providers of electronic services, or HINPs — that provide stronger safeguards than are required under PHIPA.

It is worth noting that Ontario's Freedom of Information and Protection of Privacy Act, which protects the privacy of individuals with respect to personal information held by institutions and provides a right of access to that information in accordance with specific principles[25], does not apply to PHI in[1] the custody or under the control of a health information custodian, subject to a number of exceptions [26].

PROPOSED AMENDMENTS TO PHIPA GOVERNING CONSUMER ELECTRONIC SERVICE PROVIDERS

At this time, health technology companies or commercial VCPs in Ontario that provide services to individuals at their request are not directly subject to PHIPA when they are not acting as agents of the health information custodian, as providers of electronic services or HINPs. In cases where PHIPA does not apply, PIPEDA would be the governing legislation. However, there are amendments to PHIPA that, once they come into force, may mean that some of these remaining commercial VCPs will be directly subject to PHIPA.

One of the most consequential amendments to PHIPA in relation to virtual care is that consumer electronic service providers (CESP) will be subject to PHIPA's provisions that provide individuals seeking their services with rights of access to their own PHI and the rights to correct that information. Under Ontario's PHIPA, the new amendments (which are not yet in force) define a CESP as "a person who provides electronic services to individuals at their request, *primarily* for, (a) the purpose of allowing those individuals to access, use, disclose, modify, maintain or otherwise manage their records of personal health information, or (b) such other purposes as may be prescribed" [emphasis added][27]. An example of a CESP that might fall under this definition is a health technology company that develops patient portals or digital health applications. However, not all commercial VCPs would necessarily be classified as a CESP. The proposed definition above would not necessarily apply to a commercial VCP that is not providing electronic services primarily for the prescribed purposes.

[1] These exceptions are listed in PHIPA, section 8 (1-5)

Once the new provisions are in force, a CESP will have to comply with the prescribed requirements under PHIPA, and a health information custodian that provides PHI to a CESP will also have to comply with any prescribed requirements[28]. For instance, when the amendments come into force, the Lieutenant GIC will be empowered under s. 73(1)(m.1) to make regulations that govern "the services provided by [CESPs] within the meaning of section 54.1, including their collection, use and disclosure of personal health information, the use of those services by health information custodians as well as by individuals and the rights of those individuals with regard to the services." As a result, both the services provided by the commercial VCPs as well as VCPs' handling of PHI would be covered by regulation. Since regulations are subject to less public scrutiny than legislative amendments and are more variable, this introduces considerable uncertainty about what requirements might apply when these provisions come into force. However, it is our understanding these amendments do not mean that commercial VCPs will no longer be subject to PIPEDA. They will still be subject to both PIPEDA and PHIPA, if they are an agent, a provider of an electronic service, or a HINP.

C. HOW DOES PRIVACY LAW APPLY TO VIRTUAL CARE PLATFORMS IN ALBERTA?

Alberta's health privacy legislation is unique in a number of ways. Because Alberta's PIPA has been deemed substantially similar to PIPEDA, Part 1 of PIPEDA does not apply[29]. Commercial VCPs are organizations covered by Alberta's PIPA, which means that it applies to the collection, use and disclosure of personal information by commercial VCPs. However, as mentioned, Alberta also has the HIA which applies when the personal information in question is health information[30]. To make it more complicated, because the scope of these privacy statutes depends on the nature of the activities, there will still be some health information that remains covered under PIPA. The key distinction is that personal health information that falls under the HIA is that collected, used and disclosed by health custodians when they provide a health service[31].

Commercial VCPs are not health custodians[32]. However, commercial VCPs can be affiliates of health custodians, therefore falling under the scope of the HIA. An affiliate is defined as "an individual employed by the custodian," "a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian," "a health services provider who is exercising the right to admit and treat patients at a hospital as defined in the Hospitals Act," "an information manager as defined in section 66(1)," and "a person who is designated under the regulations to be an affiliate"[33]. An affiliate of a custodian "must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian"[34]. Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be a collection, use, or disclosure by the custodian[35]. This means that commercial VCPs must walk a careful line to respect the responsibilities of a health custodian, a line that should be reflected in contractual agreements between commercial VCPs and the health custodians they work with.

The relationship between "health custodians" and their "affiliates" in Alberta's HIA echoes Ontario's PHIPA's provisions on "health information custodians" and their "agents." These provisions create a responsibility for physicians that use commercial VCPs to ensure the platforms are abiding by the law. In the Investigation into the use of Babylon by TELUS Health by Alberta physicians[36], Babylon by TELUS Health (a commercial VCP[37]) failed to meet multiple HIA requirements that protect Albertans' health privacy The physicians that provided health services through the platform under employment or contract with Babylon were held responsible for the VCP's lack of compliance. Alberta's OIPC stated that: "This investigation is an important reminder that Alberta's HIA makes custodians responsible for health information they collect, use and disclose when providing health services, whether virtually or in person. Ultimately, HIA makes the physician custodians responsible and accountable for the health information of their patients, including when they engage technology service providers both within and outside of Canada"[38].

D. CONCLUSION

The obligations of commercial VCPs under provincial health privacy laws such as Ontario's PHIPA and Alberta's HIA are somewhat different. For example, one difference between Ontario's PHIPA and Alberta's HIA is that under the latter, each custodian has a duty to prepare a privacy impact assessment when they implement a new information system or change an existing information system as it relates to the collection, use, or disclosure of health information[39]. The privacy impact assessment must be submitted to the Commissioner before implementing the new practices or changing existing systems[40], and it must describe "how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information"[41]. Theoretically, this provision would require custodians to submit a privacy impact assessment if they engage with commercial VCPs, however it is unclear how this provision is implemented. In contrast, the regulations under Ontario's PHIPA require only VCPs that are classified as HINPs to produce threat risk assessments and privacy impact assessments and provide them to the applicable health information custodians[42]. Although it is beyond the scope of this report, it is important to note that the privacy landscape is vast, so depending on how commercial VCPs conduct their business, they may be subject to privacy laws in numerous jurisdictions; if commercial VCPs rely on health custodians to comply with all governing privacy legislation, it is possible that commercial VCPs may be exposed to additional risk.

5.2 DEFINITIONS IN PRIVACY LEGISLATION

This section lays out definitions of personal information, PHI and de-identified information in PIPEDA, Ontario's PHIPA and Alberta's HIA.

A. PIPEDA

In PIPEDA, personal information is defined as "information about an identifiable individual"[43]. Courts have held that PHI is a subset of personal information for the purposes of PIPEDA[44]. In Gordon v Canada (Health) (Gordon), the Federal Court accepted the Privacy Commissioner of Canada's articulation of the applicable legal test for determining when information is about an identifiable individual: "[i]nformation will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information"[45]. This "serious possibility" test to determine when information is about an identifiable individual has been referenced and upheld in numerous decisions since Gordon, including Canada (Information Commissioner) v Canada (Public Safety and Emergency Preparedness)[46]. Another potential, albeit similar, test that has been applied by Canadian courts is the reasonable expectations test, which requires the court to consider whether there is a reasonable expectation that the individual will be identified in combination with information from other available sources[47].

Under PIPEDA, PHI refers to an individual who is living or deceased, and means "information concerning the physical or mental health of the individual," "information concerning any health service provided to the individual," "information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual," "information that is collected in the course of providing health services to the individual," or "information that is collected incidentally to the provision of health services to the individual"[48]. It is notable that there is no definition of "sensitive data" in Canada, although Principle 4.3.4 of PIPEDA does indicate that any information may be sensitive, depending on context[49].

The definition of PHI in PIPEDA is vast[50]. If commercial VCPs collect, by their virtual nature, more information "in the course of providing health services to individuals" or "incidentally to the provision of health services," they could collect more information under the PHI definition than in-person care health services. For example, since an IP address can qualify as personal information under PIPEDA when it allows for the identification of an individual[51], it could potentially qualify as PHI when collected through a commercial VCP in the course of or incidentally to the provision of health services. The OPC has not issued particular guidance aimed at commercial VCPs, so this issue remains undetermined.

PIPEDA only regulates personal information. If data is not considered personal information (for example, a de-identified dataset that cannot be linked to an identifiable individual) then it is not regulated by PIPEDA. PIPEDA does not provide a definition of de-identified information. While there is no clear definition, because personal information is information that can identify an individual, de-identified information will not constitute personal information where there is no serious possibility that an individual can be identified. In practice, it can be hard for health information custodians to distinguish between personal health information and de-identified information. For example, in PIPEDA Case Summary #2009-018[52], a psychologist considered her notes on a patient "anonymized" because they did not, from her point of view, contain sufficient information to identify the patient. These notes did not identify the name of the patient but did concern her particular case. The Commissioner noted that personal information is about an identifiable individual if there is a serious possibility that someone could identify the individual with the available information. As such, "de-identified data will not constitute 'truly anonymous information' when it is possible to subsequently link the de-identified data back to an identifiable individual"[53]. The Commissioner held that the peer review notes were about an identifiable individual, because it was possible to link the de-identified data back to the individual.

B. ONTARIO'S PHIPA

In Ontario's PHIPA, PHI, "means identifying information about an individual, in oral or recorded form, if the information,"

(a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
(c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
(d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
(e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
(f) is the individual's health number, or
(g) identifies an individual's substitute decision-maker[54].

Further, "identifying information" is defined as "information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual"[55].

There are very few rules under PHIPA governing the use, collection, and disclosure of PHI that has been de-identified.[1] In PHIPA, to de-identify "in relation to the personal health information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and 'de-identification' has a corresponding meaning"[56]. The concept of reasonable foreseeability recognizes the spectrum of de-identifiability. Section 11.2 of PHIPA prohibits using de-identified information to identify individuals, subject to certain exceptions where certain prescribed persons are permitted to re-identify information[57]. The Lieutenant GIC is empowered to make regulations "governing the de-identification of personal health information and the collection, use and disclosure of de-identified information by health information custodians and any other persons" pursuant to s. 73(1)(o.2) of PHIPA. There are no such regulations addressing de-identified data to date. As a result, there are no clear rules for when de-identified information can be used, collected, or disclosed by commercial VCPs. Of course, it is open to health information custodians to contractually ensure that commercial VCPs are not de-identifying, or using de-identified data. Though it is beyond the scope of this report, it is worth noting that there may be additional complications given that commercial VCPs in foreign jurisdictions are likely to have different interpretations of what de-identification means, resulting in further inconsistencies and creating additional risk.

C. SPECTRUM OF IDENTIFIABILITY

It is important to note that the definitions for personal information, PHI and de-identified information operate on a spectrum of identifiability, even though they operate on the idea that information is either clearly identifying or clearly non-identifying. Other jurisdictions have adopted a more nuanced approach to categorizing the spectrum of identifiability of information. The European General Data Protection Regulation (GDPR) adopts three different definitions that create a continuum of identifiability. Indeed, the GDPR recognizes "personal data" (with different levels of sensitivity that will receive proportionate protection), "pseudonymized data" and "anonymized data"[58]. Pseudonymized data is personal data that cannot be attributable to a specific individual without the use of additional information but could identify an individual if such data-matching was done. Anonymized data, on the other hand, is data that cannot, at any point using any reasonable means, identify an individual. It is possible that much of the information that is considered de-identified information in Canadian law would be considered pseudonymized data rather than anonymized data under European law.

However, as mentioned earlier, Ontario's PHIPA only reflects the spectrum identifiability through the use of "reasonably foreseeability" — for instance, "identifying information" is defined in s. 4(2) of PHIPA as information "for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual." However, Ontario is looking to introduce a better framework with regards to de-identified information (see discussion below on the Ontario White Paper).

[1] HIPA Decision 175 by the Ontario OIPC, decided in March of 2022 but published after the primary completion of this report identifies de-identification as a use within the meaning of that term in the Act, but also notes consent is not required for such use. This decision is not further addressed in this report but should be noted. Available https://decisions.ipc.on.ca/ipc-cipvp/phipa/en/item/520967/index.do.

D. ALBERTA'S HIA

The HIA does not define "personal information." Under the HIA, health information is defined as one or both of the following: "(i) diagnostic, treatment and care information; (ii) registration information"[59]. Individually identifying, in relation to health information means "the identity of the individual who is the subject of the information can be readily ascertained from the information"[60]. Under the HIA, non-identifying information "means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information"[61].

The definitions of health information are not contingent on whether the information identifies an individual or not. Regardless of whether the health information is individually identifying or non-identifying, the information in question will still be health information and therefore subject to the protections under the HIA. Another key difference with the HIA, as compared to Ontario's PHIPA and PIPEDA, is that it provides a definition for "aggregate health information," which means "non-identifying health information about groups of individuals"[62]. It also provides a definition of data-matching, which is "the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information"[63].

E. COMPARING PRIVACY LEGISLATION IN CANADA

It is hard to compare definitions across different elements of privacy legislation in Canada because the protections each Act offers varies on the scope of their application and the nature of activities they cover. This complex legal environment is a barrier for researchers and commercial actors alike.

5.3 MEANINGFUL CONSENT TO COLLECT/USE/DISCLOSE PERSONAL INFORMATION OR PHI AND DE-IDENTIFICATION

A. CONSENT UNDER PIPEDA

In the health care context, it is important to distinguish between consent to collect, use, or disclose PHI, and consent to treatment, which is outside the scope of this report. Under PIPEDA, knowledge and meaningful consent are required to collect, use, or disclose personal information[64]. This includes PHI, which is a subset of personal information. An organization may only collect, use, and disclose PHI for purposes that a reasonable person would consider appropriate in the circumstances[65]. Schedule 1 of PIPEDA outlines a number of principles that address a national standard for the protection of personal information[66]. Included in those principles is the principle of consent, which states that the "knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate"[67].

Consent is only considered valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure they are consenting to[68]. The form of meaningful consent required can vary depending on two variables: the sensitivity of the personal information and individuals' reasonable expectations[69]. Indeed, Principle 4.3.6 states organizations should seek express consent when collecting, using or disclosing sensitive personal information. Courts have recognized that PHI is almost always sensitive personal information, calling for explicit consent[70]. Therefore, when collecting, using or disclosing PHI, commercial VCPs should obtain explicit consent.

PIPEDA leaves substantial gaps however in relation to de-identified health information. For example, there are no express provisions that govern whether implied or express consent is required to use personal information to create a de-identified dataset. It is arguable that the de-identification of personal information is a use that requires consent. Further, there are no express provisions that govern what organizations can do with de- identified datasets, what a recipient of a de-identified dataset is permitted to use that dataset for, and what rules must be followed during the de-identification process.

However, PIPEDA does set out circumstances where personal information can be used without knowledge or consent. This provision permits organizations to use personal information if "it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used"[71]. Similarly, there is a provision that states that personal information can be disclosed by an organization without the knowledge or consent of the individual "for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed"[72] or "made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation"[73]. Statistical, scholarly study or research, and conservation are not defined in PIPEDA.

B. CONSENT UNDER ONTARIO'S PHIPA

In Ontario's PHIPA, there is a general requirement for consent in order to collect, use, or disclose PHI about an individual. A health information custodian must not collect, use or disclose PHI unless: "(a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or (b) the collection, use or disclosure, as the case may be, is permitted or required by this Act"[74]. Additionally, the health information custodian must "not collect, use, or disclose more [PHI] than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be"[75]. Ontario's PHIPA also includes a provision that states that health information custodians cannot collect, use, or disclose PHI about an individual for marketing purposes or "for the purpose of market research" unless the individual has expressly consented to the collection, use and disclosure of the information for those purposes[76].

In order for consent to be meaningful, the elements of consent must be established, meaning the consent: "(a) must be a consent of the individual; (b) must be knowledgeable; (c) must relate to the information; and (d) must not be obtained through deception or coercion"[77]. An individual's consent may be either express or implied[78]. However, consent must be express if "(a) a health information custodian makes the disclosure to a person that is not a health information custodian; or (b) a health information custodian makes the disclosure to another health information custodian and the disclosure is not for the purposes of providing health care or assisting in providing health care"[79]. In order for an individual to give knowledgeable consent to the collection, use, or disclosure of PHI, it must be reasonable in the circumstances to believe that the individual knows "(a) the purposes of the collection, use or disclosure, as the case may be; and (b) that the individual may give or withhold consent"[80]. In the event that an individual wants to withdraw consent, either express or implied, they can withdraw consent by providing notice to the health information custodian, however it does not have retroactive effect[81].

EXCEPTIONS TO CONSENT

Generally, PHIPA requires consent for PHI to be collected, used, or disclosed, however, there are exceptions to this rule. In particular, PHIPA permits a health information custodian to modify PHI to conceal the identity of the individual and allows the health information custodian to use PHI for research without the consent of the individual[82]. Since PHIPA allows a health information custodian to conceal the identity of an individual, information may be de-identified as long as it is in a manner consistent with Part II of PHIPA[83]. Therefore, once PHI is de-identified in the manner that falls outside of the scope of PHIPA, the de-identified information can be used and disclosed for other secondary purposes without the consent of the individual[84]. Further, health information custodians are permitted to use PHI for their own research where they meet certain requirements, including if they prepare a research plan and have a research ethics board approve that plan[85].

There are other exceptions to when PHI can be disclosed without the consent of the patient[86]. A health information custodian can disclose PHI without consent for the purposes of research, subject to certain restrictions and conditions[87]. PHIPA includes definitions for what constitutes research, a researcher, and a research ethics board. Research means "systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research"[88]. Researcher is defined as "a person who conducts research"[89]. A research ethics board is defined as "a board of persons that is established for the purpose of approving research plans [. . .] and that meets the prescribed requirements"[90].

A researcher who seeks disclosure of PHI for research purposes must submit a detailed research plan to a research ethics board for approval[91]. The research ethics board must provide a decision in writing, which sets out whether the Board approves the plan and if there are any terms and conditions for carrying out the research[92]. A health information custodian is permitted to disclose PHI about an individual to a researcher if the researcher submits an application in writing, including a research plan that must meet certain requirements, and a copy of the ethics board's decision to approve the research plan[93]. Additionally, the researcher must enter into an agreement with the health care custodian, and that agreement may impose other conditions on the researcher relating to the use, security, disclosure, return or disposal of the PHI[94]. A researcher who has an approved research plan must also comply with a number of conditions specified in s. 44(6) of PHIPA[95]. These provisions apply whether the researcher is the health information custodian themselves[96], or an outside researcher[97].

Furthermore, PHIPA grants authority to the Lieutenant GIC to make regulations that establish requirements for the means used to de-identify PHI and the collection, use and disclosure of de-identified information[98]. However, there are no regulations in relation to the de-identification of PHI at this time.

C. CONSENT UNDER ALBERTA'S HIA

INDIVIDUALLY IDENTIFYING INFORMATION: CONSENT FOR COLLECT, USE AND DISCLOSURE

Under the HIA, custodians are only able to collect individually identifying health information if the collection of the information is expressly authorized by an enactment of Alberta or Canada, or "if that information relates directly to and is necessary to enable the custodian to carry out a purpose that is authorized under section 27," which sets out the purposes for which individually identifying health information can be used[99]. Permitted uses of individually identifying health information under section 27 of HIA include, but are not limited to: providing health services; determining or verifying the eligibility of an individual to receive a health service; conducting investigations, discipline proceedings, practice visits or inspections that relate to members of a health profession or health discipline; conducting research or performing data matching or other services in order to facilitate another person's research; providing health services provider education; carrying out any purpose that is authorized by an enactment of Alberta or Canada; or for internal management purposes[100]. Other permitted uses of individually identifying information include: planning and resource allocation; health system management; public health surveillance; and health policy development. Custodians are permitted to "strip, encode or otherwise transform individually identifying health information to create non-identifying health information"[101]. Under the HIA, a custodian is allowed to disclose individually identifying information without the individual's consent to another custodian[102]. Therefore, a health custodian could theoretically allow a commercial VCP acting as its affiliate to disclose individually identifying information to another custodian, or its affiliate[103].

Health custodians are also permitted to use individually identifying health information, subject to certain qualifications, for "conducting research or performing data matching or other services to facilitate another person's research"[104]. For example, in order to conduct research, the health custodian or researcher must have submitted a research protocol to a research ethics board[105]. A custodian who has received a written application may, but is not required to, disclose the health information or perform data matching or other services to facilitate the research proposal[106].

If the health custodian does decide to disclose the health information, perform the data matching or other services to facilitate research, then the researcher must enter into an agreement with the custodian where the researcher must agree to comply with the HIA and agree to any other condition that the custodian imposes on them relating to safeguarding against the identification of an individual who is the subject of the information[107]. If the researcher contravenes or fails to comply with the conditions set out by the research ethics board or the custodian, then the agreement is canceled, and the researcher "is no longer authorized to use the health information for any purpose and must destroy the health information or return it to the custodian"[108].

A health custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure[109]. Theoretically, this means that if a patient consents to the collection, use or disclosure of individually identifying health information to a commercial VCP, then a health custodian would be permitted to provide that VCP with the information. This consent must respect several conditions and can be revoked in writing or electronically[110]. However, there are several specific situations where consent does not need to be obtained for a custodian to disclose individually identifying diagnostic, treatment, and care information[111]. This includes situations where the custodian believes, on reasonable grounds, that the disclosure will avert or minimize (i) a risk of harm to the health or safety of a minor, or (ii) a significant risk of harm to the health or safety of any person[112].

NON-IDENTIFYING INFORMATION: CONSENT FOR COLLECT, USE AND DISCLOSURE

Under the HIA, a health custodian is able to collect, use, and disclose non-identifying health information for any purpose[113]. Custodians are permitted to "strip, encode or otherwise transform individually identifying health information to create non-identifying health information"[114]. Therefore, health custodians are able to de-identify information without consent for any purpose. As stated earlier, a health custodian is permitted to use identifiable information for research purposes, if that plan meets the criteria set out in the HIA[115]. If a disclosure of non-identifying health information is made to a person other than another custodian, then the custodian "must inform the person that the person must notify the Commissioner of an intention to use the information for data matching before performing the data matching"[116]. This means that if non-identifying health information were provided to a commercial VCP, then the VCP would have an obligation to notify the Commissioner of any intention to use that information for data matching, prior to performing the data matching.

5.4 ROLE OF REGULATORY COLLEGES IN THE DE-IDENTIFICATION OF PHI

While there is no indication that regulatory colleges have created or enforced guidelines or standards in relation to the de-identification of PHI, regulatory colleges might be a potential avenue for creating oversight to de-identification standards and practices. There is nothing in PHIPA or the HIA that would interfere with a regulatory college's ability to set professional standards or prohibit the de-identification of PHI. The ability of each college to regulate the de-identification of PHI would turn on its specific mandate and jurisdiction, which will not be considered in this report. Legislative reform, however, is preferable to implementing varied standards through independent regulatory colleges in order to ensure that standards are both robust and uniform across health care professions.

A. ONTARIO'S PHIPA

Under PHIPA, there is a provision that stipulates that nothing in the statute interferes with "the regulatory activities of a College under the Regulated Health Professions Act, 1991, the College under the Social Work and Social Service Work Act, 1998 or the Board under the Drugless Practitioners Act"[117]. It appears that regulatory colleges are not barred by PHIPA from introducing rules or guidelines that govern the de-identification of PHI. For instance, pursuant to the Regulated Health Professions Act, colleges have as their object "[t]o develop, establish and maintain programs and standards of practice to assure the quality of the practice of the profession," and to do so in a manner that serves and protects the public interest[118]. In carrying out this duty, it may be open to a college to establish rules or guidelines that govern de-identification, or prohibit health information custodians that fall under their jurisdiction from de-identifying PHI altogether.

Similarly, under s 44(5) of PHIPA, health information custodians have the discretion to impose conditions on researchers' "use, security, disclosure, return or disposal of the information"[119]. As a result, there is no impediment under PHIPA to a health information custodian complying with any additional professional/college guidelines/rules.

B. ALBERTA'S HIA

Under HIA, nothing prohibits colleges from establishing rules and guidance with respect to de-identifying information. Unlike in Ontario's PHIPA, there are no clear provisions that stipulate that nothing in the statute interferes with the Health Professions Act[120]; however, there is a provision that states "[a] custodian that collects, uses or discloses health information pursuant to another enactment must comply with this Act"[121]. It appears that regulatory colleges have the power to enact provisions that regulate the de-identification of PHI and/or prohibit custodians from de-identifying PHI, as it relates to their role of "[providing] direction to and regulat[ing] the practice of the regulated profession by its regulated members"[122].

Similarly, under section 53(1) of the HIA, health custodians have the discretion to choose whether health information, data matching, or other services will be provided to the researcher, when that research has been approved by the research ethics board. If a custodian does choose to supply the information to the researcher, they are permitted to impose their own conditions on the use of the information, including obtaining consent from the individuals and requiring the researcher to allow access to the research premises to ensure that the researcher is complying with the HIA[123].

5.5 AUDIT/INVESTIGATIONS

Unfortunately, publicly available information indicates that audits are not routinely conducted by the OPC[124], Ontario OIPC [125], or the Alberta OIPC[126]. It appears that most, if not all, of the investigations that are conducted by these agencies are prompted by a breach report or privacy complaint. This is problematic as compliance with the jurisdictionally relevant legislation by commercial VCP's is up to the organizations and is not meaningfully subject to proactive oversight unless there has been a complaint from the public. Due to the complex relationship between federal and provincial privacy legislation, it is possible that commercial VCPs might not be aware of what laws their actions are subject to. This may result in sensitive personal information, including PHI, being less protected than it should be by law.

5.6 POSSIBLE DEVELOPMENTS IN CANADA PRIVACY LAWS IMPACTING VCPS

A. BILL C-11: AN OVERALL STEP BACK FOR PRIVACY

The proposed Consumer Privacy Protection Act (Bill C-11) was meant to replace PIPEDA in the Canadian privacy landscape[127]. Although government may introduce similar legislation at some point in the future, Bill C-11 did not make it past its first reading in the House of Commons on 17 November 2020. Bill C-11 addressed some of the questions concerning the privacy protection of personal information, PHI, and de-identified information. The legislation permitted the use of de-identified information, independently of its sensitivity, for internal business purposes[128]. Disclosures of de-identified information would have been permitted for socially beneficial purposes to governments, health care institutions or other organizations that are government mandated to "carry out a socially beneficial purpose"[129]. The socially beneficial purpose included any health related purposes[130]; therefore, it could have enabled public-private partnerships between governments and commercial VCPs, such as the one the Alberta government developed with the VCP Babylon by Telus Health in 2020[131].

The provision in C-11 permitting de-identification has been criticized for not having sufficient safeguards[132]. It had the potential to enable a significant range of de-identified information disclosures on the grounds of being "socially-beneficial," begging the question of whether every application in the area of health is genuinely "socially beneficial" or who gets to decide whether or not any given use of data would meet that threshold. Many questions were left unanswered: would the privacy interests of the individuals be taken into account in determining what purposes were socially beneficial? Would there be oversight to verify the socially beneficial nature of the purposes? Such legal gaps were present throughout the legislation, prompting Privacy Commissioner Daniel Therrien to describe Bill C-11 as "a step back overall for privacy"[133].

B. ONTARIO'S 2021 WHITE PAPER

Another recent initiative is the Government of Ontario's June 17, 2021 White Paper titled "Modernizing Privacy in Ontario"[134]. It is still unknown if the White Paper's proposals will lead to legislative change, or how the proposed laws might interact with PHIPA; it should be noted that the Ontario OIPC has urged the Government of Ontario to press forward with implementing it even if Bill C-11 is no longer in the legislative process at the federal level[135]. The White Paper does not specifically address the particularities of commercial VCPs; however, if the proposals were enforced, commercial VCPs would naturally be subject to more oversight and greater obligations as would other organizations. The White Paper is divided under key areas of reform: rights-based approach to privacy; safe use of automated- decision making; enhanced consent and other lawful uses of personal data; data transparency for Ontarians; a fair, proportionate and supportive regulatory regime; and support for Ontario innovators. All these areas of reform have the potential to affect the way commercial VCPs collect, use, and disclose PHI.

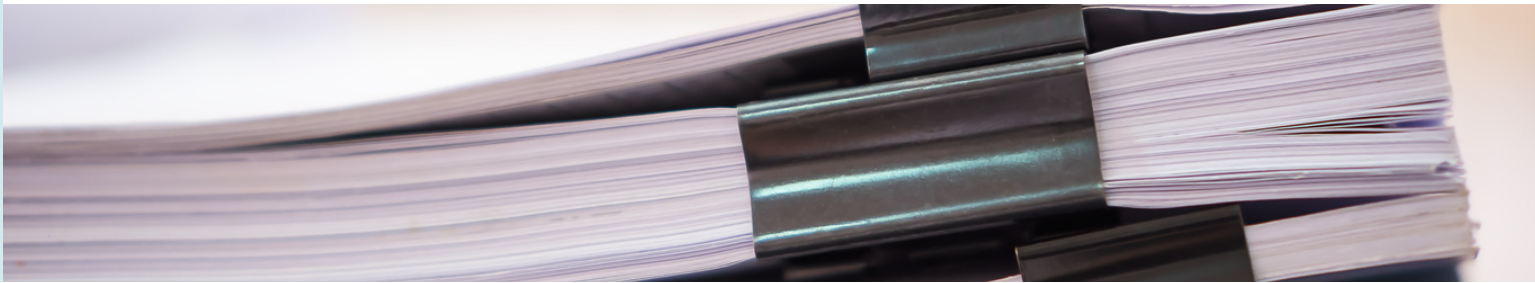
Under the "rights-based approach to privacy" reform area, the Government of Ontario wishes to establish a fundamental right to privacy and considers doing so by proposing language for various provisions that would need to be introduced by the legislature[136]. These provisions recognize the fundamental right to privacy, which would strengthen Ontario's privacy protections. Ontario is also looking to create an overarching provision that stipulates information can only be collected, used and disclosed for purposes that an individual would reasonably expect, regardless of which lawful grounds for collecting, using and disclosing personal information may apply[137]. Therefore, even when a commercial VCP would have legal grounds to collect personal information or PHI, it may have to obey the "legitimate and fair purpose" criterion[138]. Many factors would be taken into account to evaluate the purposes, for example the sensitivity of the information or whether the information is de-identified[139]. These factors would affect commercial VCPs, as PHI is a significant part of the data they collect and courts have held that PHI is almost always considered sensitive information[140]. It is unclear how such provisions would interact with PHIPA, which provides in s. 4(3) that all personal identifying information in mixed records — records that contain both identifying information (that is not PHI) and PHI — is to be treated as PHI.

The White Paper also introduces automated-decision system (ADS) guardrails[141]. For example, if commercial VCPs were to use ADS to classify the priority of patients according to symptoms and demographics, on the request of the individual, they would have to provide an explanation of the prediction, recommendation, or decision, and of how the personal information used was obtained[142]. The individuals subject to this ADS would have access to the information used in the system and would be allowed to request the correction of their information, to comment on their information, to contest it as well as to ask for a person to review it[143]. Ontario is also considering a provision that would prohibit commercial VCPs (and other organizations) from using ADS when the decisions taken would have a significant impact on individuals[144].

Under the "data transparency" section, the main proposal is mandating a privacy management program for organizations[145]. The level of complexity of the privacy program would be proportional to the volume, nature and sensitivity of the personal information dealt with by the organization[146]. Commercial VCPs deal with sensitive information, which implies they would have to develop more complex and comprehensive privacy program[147]. The programs would be required to be publicly available in plain language[148].

Finally, a number of measures are considered to enhance Ontario's privacy regulatory regime[149]. This area of reform would not impose more obligations on commercial VCPs but creates more incentives to meet the ones mentioned above. Firstly, it would give the Ontario OIPC and the Ministry of Government and Consumer Services responsibilities to develop guidance material on compliance, not without recognizing the Ontario OIPC has been fulfilling this role for years[150]. Secondly, it could give the Ontario OIPC the role of developing and issuing "codes of practice" that would work as certification for compliance with the new legislation. Thirdly, the Ontario OIPC could have the authority to apply the law through binding orders, conduct investigations and audits, issue orders to cease an illicit activity and orders to destroy personal information that was collected unlawfully[151]. Lastly, provisions set out parameters for monetary penalties that would be administered[152] by the Ontario OIPC. The maximum administrative penalty contemplated for an organization that is not an individual is noted as $10,000,000.00, or 3% of the organization's global revenue in the financial year prior to the penalty being imposed[153].

Throughout the White Paper, strengthened privacy provisions tend to encourage organizations to use de-identified information, as opposed to identifying information. For example, under the "enhancing consent" reform area, the White Paper suggests allowing organizations to disclose an individual's information without obtaining consent if, among other conditions, it is de-identified[154]. Additionally, whether or not the information is de-identified is a factor that is taken into account in the evaluation of the "legitimate and fair purpose" criterion[155]. Other areas of reform, such as the "supporting Ontario innovators" section, uses stronger language, stating Ontario would at times require that organizations de-identify personal information[156]. The White Paper also suggests applying certain privacy rules to de- identified information, acknowledging there are risks of re-identification[157]. These rules would be, namely, the implementation of a privacy program ensuring security protections for de-identified data (that have yet to be specified), and providing an opportunity to make a complaint or request information on the privacy program's compliance with the law[158]. Re-identification would also be prohibited, except in accordance with certain measures set out in law[159]. The White Paper also offers insights on the administrative and technical definition of de-identified data, which has proven to be controversial because of the risk of re-identification[160]. The de-identification protocols that Ontario would adopt would require organizations to ensure that the de-identification is proportionate to the sensitivity of the personal information handled[161]. Again, because commercial VCPs are dealing with sensitive information, it would likely be expected that they put in place stringent de-identification protocols. Finally, the White Paper suggests introducing, for the first time in Canadian law, the European notion of "anonymized data," which is defined as data that has been altered irreversibly, according to generally accepted best practices, in such a way that no individual could be identified from the information, whether directly or indirectly by any means or by any person[162]. This category of data that would not be subject to any privacy protection.



References

1. *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5 [PIPEDA]. Note that privacy law is an evolving field– the information contained in this report is, to the best of the authors' knowledge, accurate as of 29 March 2022.
2. Industry Canada, *PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector: Questions & Answers*, (Ottawa: Industry Canada, 25 February 2013) at 3.
3. PIPEDA, s*upra* note 1 at s 26(2)(b).
4. Office of the Privacy Commissioner of Canada, *Report to Parliament on Substantially Similar Provincial Legislation*, (Ottawa: Minister of Public Works and Government Services Canada, 2002).
5. *Ibid*.
6. Department of Industry, (2001) C Gaz I, 3621-3622 (PIPEDA).
7. *An Act respecting the protection of personal information in the private sector*, RSQ, c P-39.1. See also the GIC's exemption order: *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374. This Act will be replaced by Bill-64, *An Act to Modernize Legislative Provisions respecting the Protection of Personal Information*, 1st Sess, 42nd Leg, Quebec, 2020 (sanction September 22, 2021), SQ 2021, c 25 (assented to 22 September).
8. *Personal Information Protection Act*, SBC 2003, c 63. See also the GIC's exemption order: *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220.
9. *Personal Information Protection Act*, SA 2003, c P-6.5 [Alberta Exemption Order]. See also the GIC's exemption order: *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219.
10. *Personal Health Information Protection Act, 2004*, SO 2004, c 3 [PHIPA]. See also the GIC's exemption order: *Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399.
11. *Personal Health Information Privacy and Access Act,* SNB 2009, c P-7.05. See also the GIC's exemption order: *Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265.
12. *Personal Health Information Act,* SNS 2010, c 41. See also the GIC's exemption order: *Personal Health Information Custodians in Nova Scotia Exemption Order,* SOR/2016-62.
13. *Personal Health Information Act,* SNL 2008, c P-7.01. See also the GIC's exemption order: *Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72.
14. *Health Information Act,* RSA 2000, c H-5 [HIA].
15. *Ibid* at s 1(2).
16. PHIPA, *supra* note 10 at ss 2-3 [emphasis added].
17. *Ibid* at s 3(1)(1).
18. *Ibid* at s 17(3).
19. *Ibid* at s 17(2). Subsection 17(1) provides that a health information custodian is responsible for PHI in its custody and control and may permit the custodian's agent to collect, use, disclose, retain or dispose of PHI on the custodian's behalf if it is required by the custodian; if it is necessary in the course of the agents duties; and if the prescribed requirements are met. Subsection 17(1.1) provides that the custodian can subject this permission to conditions or restrictions on the agent.
20. *Ibid* at s 17(4).
21. General, O. Reg. 329/04, s. 6.
22. General, O. Reg. 329/04, s. 6(1).
23. General, O. Reg. 329/04, s. 6(2).
24. General, O. Reg. 329/04, s. 6(3).
25. Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31, s. 1.
26. PHIPA, s. 8
27. PHIPA, supra note 10 at s 54.1(1) (not yet in force).
28. Ibid at s 54.1(2) (not yet in force).
29. Alberta Exemption Order, supra note 9 at s 1.
30. HIA, supra note 14 at s 5(1).
31. Ibid at s 1(2).
32. Ibid at s 1(1)(f). HIA designated custodians are, for the most part, positions established by other Alberta legislation governing the health sector, which do not apply to VCPs. The full definition of custodian is as follows:

> 1.(1) (f) "custodian" means:
> (i) the board of an approved hospital as defined in the Hospitals Act other than an approved hospital that is
> (A) owned and operated by a regional health authority established under the Regional Health Authorities Act, or
> [...]
> (ii) the operator of a nursing home as defined in the Nursing Homes Act other than a nursing home that is owned and operated by a regional health authority established under the Regional Health Authorities Act;
> (ii.1) an ambulance operator as defined in the Emergency Health Services Act;
> (iii) a provincial health board established pursuant to regulations made under section 17(1)(a) of the Regional Health Authorities Act;
> (iv) a regional health authority established under the Regional Health Authorities Act;
> (v) a community health council as defined in the Regional Health Authorities Act;
> (vi) a subsidiary health corporation as defined in the Regional Health Authorities Act;
> [...]

(viii) a board, council, committee, commission, panel or agency that is created by a custodian referred to in subclauses (i) to (vii), if all or a majority of its members are appointed by, or on behalf of, that custodian, but does not include a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the Alberta Evidence Act; (ix) a health services provider who is designated in the regulations as a custodian, or who is within a class of health services providers that is designated in the regulations for the purpose of this subclause;
(ix.1) the Health Quality Council of Alberta;
(x) a licensed pharmacy as defined in the Pharmacy and Drug Act;
[...]
(xii) the Department;
(xiii) the Minister;
(xiv) an individual or board, council, committee, commission, panel, agency, corporation or other entity designated in the regulations as a custodian.

33. Ibid at s 1(1)(a).
34. Ibid at s 28.
35. Ibid at s 62(2).
36. Office of the Information and Privacy Commissioner of Alberta, Investigation Report H2021-IR-01: Investigation into the use of Babylon by TELUS Health by Alberta physicians (Alberta: 29 July 2021), online: <https://www.oipc.ab.ca/media/1165671/h2021-ir-01.pdf> [Babylon Telus Investigation].
37. The Alberta OIPC found that Babylon and the physicians failed to meet their obligations under the HIA with respect to every issue that was investigated. In doing so, the Alberta OIPC found that the physicians failed to establish or adopt policies and procedures that would facilitate the implementation of the HIA, to prepare a privacy impact assessment that would be useful to mitigate the confidentiality and privacy risk and to submit it to the OIPC, to enter into an information manager agreement with Babylon, to meet the requirements of the HIA with respect to health information that is stored or used by a person in a jurisdiction outside Alberta, to provide administrative and technical safeguards for the protection of health information, and to collect, use and disclose health information in a limited manner. See: Babylon Telus Investigation, supra note 30 at 65.
38. Ibid at 4.
39. HIA, supra note 14 at s 64(1)-(2).
40. Ibid at s 64(2).
41. Ibid at s 64(1).
42. General, O. Reg. 329/04, s. 6(3).
43. PIPEDA, supra note 1 at s 2(1).
44. Rousseau v Wyndowe, 2008 FCA 39, [2008] FCJ No 151, at para 42 [Rousseau].
45. 2008 FC 258, 173 ACWS (3d) 667 at para 34 [Gordon].
46. 2019 FC 1279, 315 ACWS (3d) 395 at para 35.
47. See Canada (Information Commissioner) v Canadian Transportation Accident Investigation & Safety Board, 2006 FCA 157, [2006] FCJ No. 704 at para 43.
48. PIPEDA, supra note 1 at s 2(1).
49. PIPEDA, supra note 1 at Schedule 1, s. 4.3.4.
50. Ibid.
51. Office of the Information and Privacy Commissioner of Canada, What an IP Address Can Reveal About You, (Ottawa: Technology Analysis Branch, 2013) at 3, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/>.
52. Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2009-018: Psychologist's anonymized peer review notes are the personal information of the patient, (23 February 2009), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-018/>.
53. Ibid.
54. PHIPA, supra note 10 at s 4(1).
55. Ibid at s 4(2).
56. Ibid at s 2.
57. PHIPA, s. 11.2(2).
58. EC, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 at Recital 26, and Articles 4(1), (5).
59. HIA, supra note 14 at s 1(1)(k).
60. Ibid at s 1(1)(p).
61. Ibid at s 1(1)(r).
62. Ibid at s 57(1).
63. Ibid at s 1(1)(g).
64. PIPEDA, supra note 1 at Principle 3.
65. Ibid at s 5(3).
66. Ibid at Schedule 1.
67. Ibid at Schedule 1, 4.3 Principle 3.
68. Ibid at s 6.1.

69. Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2003-207: Cellphone company meets conditions for "opt-out" consent, (6 August 2003), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-207/>. See also Ibid at Schedule 1, Principles 4.3.4 and 4.3.5.
70. Townsend v Sun Life Financial, 2012 FC 550, 217 A.C.W.S. (3d) 516 at para 25.
71. PIPEDA, supra note 1 at s 7(2)(c).
72. Ibid at s 7(3)(f).
73. Ibid at s 7(3)(g).
74. PHIPA, supra note 10 at ss 29(a)-(b).
75. Ibid at s 30(2).
76. Ibid at s 33.
77. Ibid at s 18(1).
78. Ibid at s 18(2).
79. Ibid at s 18(3).
80. Ibid at s 18(5).
81. Ibid at s 19(1).
82. Ibid at ss 37(1)(f), (j).
83. Ibid, s 37(1)(f).
84. Information and Privacy Commissioner of Ontario, "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy," (June 2011), online: <https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf> at 10.
85. PHIPA, supra note 10, s 37(1)(j). This provision is also subject to PHIPA subsections 44 (2) to (4) and clauses 44(6)(a)-(f) apply to the use as if it were a disclosure.
86. Ibid at ss 38-50.
87. Ibid at ss 44(1)-(11).
88. Ibid at s 2.
89.Ibid.
90.Ibid.
91. Ibid at s 44(1)(a)(iii), (2), (3)(a)-(d). Pursuant to s 44(3)(a)-(d), the Board must consider:

> (a) whether the objectives of the research can reasonably be accomplished without using the personal health information that is to be disclosed;
> (b) whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose personal health information is being disclosed and to preserve the confidentiality of the information;
> (c) the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal health information is being disclosed; and
> (d) whether obtaining the consent of the individuals whose personal health information is being disclosed would be impractical.

92. *Ibid* at s 44(4).
93. *Ibid* at ss 44(1)-(2).
94. *Ibid* at s 44(5).
95. *Ibid* at s 44(6). This includes the following conditions: the researcher must use the PHI only for purposes set out in the research plan; not publish any information that could reasonably enable a person to ascertain the identity of the individuals; not disclose the information except as required by law; not contact the individuals unless the health information custodian obtains the individuals' consent to being contacted; notify the custodian of any breaches; and comply with the agreement respecting disclosure.
96. *Ibid* at s 37(3).
97. *Ibid* at s 44(1).
98. *Ibid* at s 73(1)(o.2).
99. HIA, *supra* note 14 at s 20(b).
100. *Ibid* at s 27(1).
101. *Ibid* at s 65.
102. *Ibid* at s 35(1)(a)(k).
103. *Ibid* at s 43.
104. [1] *Ibid* at s 27(d). Under the HIA, research is defined as "academic, applied or scientific research that necessitates the use of individually identifying health information." See, *ibid* at s 1(1)(v).
105. *Ibid* at s 27(1)(d)(i)-(v). The research ethics board must be satisfied that the research protocol meets the criteria set out in the HIA; the custodian or researcher must comply with conditions that are suggested by the research ethics board; and if the research ethics board recommends that consent of the individuals is required for this research, then consent must be obtained.
106. *Ibid* at s 53(1).
107. *Ibid* at s 54(1)(a).The researcher must also agree to use the health information only for the purposes in the research protocol; not publish the health information in a form that might reasonably enable the re-identification of the individual; not contact any individual who is the subject of the information, unless that person has consented to be contacted; to allow the custodian to access or inspect the researchers premises to ensure that the researcher is complying with its obligations; and to pay the costs, as required. See *ibid* at s 54(1)(b)-(f).
108. Ibid at s 54(4)(b).
109. Ibid at s 34(1). This provision is subject to ss 35 and 40.

110. Ibid at s 34(2)-(6).
111. Ibid at s 35(1).
112. Ibid at s 35(m).
113. Ibid at ss 19, 26, 32(1).
114. Ibid at s 65.
115. Ibid at s 27(1)(d).
116. Ibid at s 32(2).
117. PHIPA, supra note 10, at s 9(2)(e). This sub-section will be repealed and substituted with the following provision:
(e) the regulatory activities of a College under the Regulated Health Professions Act, 1991, the College under the Social Work and Social Service Work Act, 1998, the Board under the Drugless Practitioners Act or the Health and Supportive Care Providers Oversight Authority under the Health and Supportive Care Providers Oversight Authority Act, 2021.
This is to be done "[o]n a day to be named by proclamation of the Lieutenant Governor."
118. Regulated Health Professions Act, 1991, SO 1991, c 18, ss 3(1)3, (2).
119. PHIPA, supra note 10 at s 44(5).
120. HIA, supra note 14 at s 33(4). See also Health Professions Act, RSA 2000, c H-7 [HPA].
121. Ibid at s 6.
122. HPA, supra note 112 at s 3(1)(b).
123. HIA, supra note 14 at s 54(1)(a) and (e).
124. Office of the Privacy Commissioner of Canada, "Audits," online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/>. There are only seven publicly available audits on the OPC website. None of these audits related to commercial entities in the health sector dealing with PHI.
125. The Information and Privacy Commissioner of Ontario has the authority to conduct self-initiated reviews under PHIPA (see, PHIPA, supra note 10 at s 58(1)). However, in the IPC's response to an email inquiry about whether the IPC conducts self-initiated reviews, the IPC stated that it does not randomly investigate health information custodians and that in general, a breach report or privacy complaint would trigger the audit or investigation process. Email from Information and Privacy Commissioner of Ontario to Leslie Schumacher and Béatrice Allard (15 December 2021). Email on file with the authors.
126. Under section 84(1)(a) of HIA, supra note 14, the Commissioner is permitted to open investigations into compliance with the HIA. Most of the investigations that are available on the website appear to be prompted by reports of privacy breaches by the health custodians or complaints submitted by the general public. Since 2015, there are seven available investigation reports that relate to health organizations and health custodians. Six of those investigations fell under the HIA. See: Office of the Information and Privacy Commissioner of Alberta, "Investigation Reports," online: OIPC <https://www.oipc.ab.ca/decisions/investigation-reports.aspx>.
127. Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 2nd Sess, 43 Parl, s 21 [Bill C-11].
128. Ibid at s 21.
129. Ibid at s 39(1).
130. Ibid at s 39(2).
131. See Government of Alberta, "New app helps Albertans access health care," March 19, 2020. Available: https://www.alberta.ca/release.cfm?xID=69851809AA1B8-AEA8-D268-E2D1E54D6DF119C0. See also, Alberta OIPC, "Commissioner releases Babylon by Telus Health Investigation Reports," July 29, 2021. Available: https://www.oipc.ab.ca/news-and-events/news-releases/2021/babylon-by-telus-health-reports-released.aspx
132. Teresa Scassa, "Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill," (6 December 2020) online (blog): <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=335:data-for-good?-an-assessment-of-the-proposed-exception-in-canada%E2%80%99s-private-sector-data-protection-law-reform-bill&Itemid=80>.
133. Office of the Information and Privacy Commissioner of Canada, "Commissioner: Reform bill "a step back overall" for privacy" (11 May 2021), online (blog): <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210511/>.
134.Government of Ontario, Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy: WHITE PAPER (2021), online (pdf): <https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462> [White Paper].
135. Patricia Kosseim, "IPC Comments on the Ontario's Government Modernizing Privacy in Ontario," (Toronto: Information and Privacy Commissioner of Ontario, 2021) at 2, online: <https://www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-ipc-comments-on-gov-white-paper_modernizing-privacy-in-ontario.pdf>.
136. White Paper, supra note 125 at 3-4.
137. Ibid at 5.
138. Ibid at 6-7.
139. Ibid.
140. Townsend v Sun Life Financial, supra note 62, at para 25
141.White Paper, supra note 125 at 11.
142. Ibid at 13.
143. Ibid at 14.
144. Ibid at 13-14.
145. Ibid at 25.
146. Ibid at 26.
147. Ibid at 26.
148. Ibid at 27.

149. Ibid at 33.
150. Ibid at 34.
151. Ibid at 5.
152. Ibid at 34-36.
153. Ibid at 36. Additionally, for organizations that are individuals the maximum administrative penalty would be $50,000.00.
154.Ibid at 5.
155. Ibid.
156. Ibid at 39.
157. Ibid at 40.
158. Ibid.
159. Ibid.
160. Ibid.
161. Ibid.
162. Ibid at 41.

SECTION 6: DISCUSSION

In this analysis, we explored the privacy implications of the direct-to-patient commercial virtual care industry in Canada, a complex jurisdictional landscape. We found that many VCP companies engage in widespread collection, commercial use and, in some cases, sharing of sensitive health-related information. Problematically, some commercial VCPs appear to be using data to influence patient health care journeys, with the goal of increasing uptake of a business partner's pharmaceutical products. Additionally, company privacy policies and terms of service documents are confusing, vague and do not adequately convey how data might be used by third parties. Patients are often required to agree to many commercial uses of their data, unnecessary for clinical care, prior to being able to access health services. These data uses often serve a company's business interests. Finally, as companies view patient data as a proprietary asset, data may not be available to public and non-profit entities for research and health system improvement.

PRIVACY LEGISLATION AND REGULATION

Our legal analysis indicates that commercial VCPs operate in a complex jurisdictional landscape. Federal privacy legislation enacted in 2000, PIPEDA, specifically covers the collection, use or disclosure of personal information for commercial reasons[1]. PIPEDA applies to various subsets of personal information including PHI. As PIPEDA is a national statute, it applies to all provinces, except when a province or a specific sector of the province is covered by a provincial privacy statute is "substantially similar" to PIPEDA; then, the specific activities, organizations or class of organizations that are covered by the exemption order will not be subject to PIPEDA. For example, Québec, British Columbia and Alberta have private sector privacy legislation that have been deemed substantially similar to PIPEDA[2–4]. The exemption orders granted to these provinces free their organizations from applying PIPEDA to any collection, use and disclosure of personal information. Additionally, Ontario (Ontario PHIPA), New Brunswick, Nova Scotia, and Newfoundland and Labrador have received an exemption from PIPEDA for their health privacy laws, which exempt health information custodians from complying with Part I of PIPEDA in respect of the collection, use, and disclosure of PHI[5–8].

As a result, in provinces where health custodians have an exemption from PIPEDA, commercial VCPs fall under the provincial health privacy legislation when they collect, use and disclose PHI as providers of electronic services, or as "agents" (under Ontario's PHIPA) or "affiliates" (under Alberta's HIA) of health custodians[9]. However, commercial VCPs fall under PIPEDA's jurisdiction when they collect, use, and disclose PHI for commercial activities (such as marketing, improving customer experience and other business purposes). (Planned amendments to the Ontario's PHIPA legislation will introduce provisions that would make commercial VCPs directly subject to the provincial statute[10].) In other provinces and territories, commercial VCPs' activities are regulated solely by PIPEDA.

Our analysis suggests that some VCP companies and health custodians may not be fully aware of the complex cross-jurisdictional legal framework in which they operate. Guidance issued by the Ontario IPC in February 2021 provided additional details on how VCPs, both those that are considered agents and those considered non-agents, should act in order to comply with the legislation[11]. Moreover, the investigation by the Alberta OIPC into Alberta physicians' use of Babylon by TELUS Health demonstrates that health custodians who operate health services through VCPs may not understand they have an obligation to verify the compliance of these platforms with privacy legislation when these platforms act as their agents or affiliates (Box 1)[12].

Adding on this complex jurisdictional governance landscape, audits are not routinely conducted by the OPC, Ontario OIPC, or the Alberta OIPC[12]. These could serve as valuable educational tools to VCP companies and custodians. From our analysis, it appears that most, if not all, of the investigations that are conducted by these agencies are prompted by a breach report or privacy complaint. This is problematic as commercial VCPs' compliance with provincial and federal privacy legislation is monitored internally within the organizations and is not subject to proactive, external oversight. Due to the complex relationship between federal and provincial privacy legislation, VCP companies may not be aware of the applicable legislation. As a result, sensitive personal information, including PHI, is less protected than the law provides for and patients expect.

GAPS IN CANADIAN HEALTHCARE SYSTEMS

Our analysis provides insight into gaps in Canadian health systems. Study participants described commercial VCPs as solving problems in the Canadian healthcare system by improving access to care and by diverting visits from overwhelmed emergency departments. These are real shortcomings in the health system. Many Canadians lack a primary care provider, and those who have one often struggle to get timely access[13]. In a 2016 Canadian study of emergency department patients, 47% chose to visit the emergency department because they could not get an appointment with their primary care provider[14]. Newly published Canadian research, however, indicates that patients who use a commercial VCP are more likely to have an emergency department visit in the next thirty days as compared to a patient who has a virtual visit with their regular primary care provider[15], indicating a need to more closely examine the commercial model of virtual care.

Many participants in our study positioned commercial VCPs as a viable and legitimate solution to the gaps. They believed that commercial virtual care, as part of the private sector, viewed patients as consumers and were more responsive to their needs than the public sector. The emergence of commercial virtual care, therefore, may be creating a shift from health systems taking responsibility for the well being of a population, to patients as consumers, responsible for their individual care journeys. Participants also promoted the narrative that the public sector was unable to create as efficient and innovative solutions as the private sector. Participants recommended some adjustments to the commercial model, including improved data sharing between entities, increased public funding and enhanced regulation. However, our analysis identifies privacy-related concerns with commercial VCPs, such as the collection, use and sharing of sensitive health-related data, issues that may be fundamental to the existing model of commercial virtual care.

NARROWING THE DEFINITION OF PHI

Our analysis indicates that many VCP companies engage in widespread collection, commercial use and, in some cases, sharing of health-related information. According to participants and VCP company documents, this is enabled by a narrow definition of PHI. Platforms generally defined PHI as the data collected when a participant interacted with a physician, nurse practitioner, or other regulated health professional. Platforms considered other data they collected during sign-up or registration, such as an individual's name, email address, and IP address, as personal information, but not PHI. Personal information often receives different legal protections than PHI and is typically considered a less sensitive form of data than PHI by the public[16–18]. Thus, this distinction between the two types of data appeared to permit commercial uses of information that VCP companies exclude from the PHI category. In some cases, VCP companies not only used this sign-up/registration information internally for commercial reasons but also shared it with the other subsidiaries within the corporation, externally with business partners or with companies seeking to place advertisements on the platform.

Excluding sign-up/registration data from the PHI category, however, does not reflect the nature of these data. Since commercial VCPs are providing a health service, the sign-up/registration information is by nature PHI. Accordingly, the federal privacy legislation, PIPEDA, defines PHI as information collected as part of or "incidentally" during the provision of health services[19]. To date, however, the OPC has not issued guidance aimed directly at commercial VCPs. Alberta's HIA, however, specifically mentions registration information, effectively including it in the definition of "health information" under that Act[20]. If commercial VCPs are adopting an internal definition of PHI that is narrower than the legal definitions of PHI, a portion of patients' information that should be legally protected as PHI is not.

SHARING DATA WITH DATA BROKERS

Participants and company documents described how commercial VCPs often collected and shared user information (e.g., IP addresses, geolocation information, and device identifiers and browsing information) with data brokers, like Google or Facebook, for data analytics. These data were sometimes described as unidentified or non-personal information because they did not contain names, implying that data were exempt from most privacy legislation. However, these data can often identify a unique individual, particularly when shared with a data broker[21]. Data brokers use data-matching methods (e.g., cookie syncing, device fingerprinting, probabilistic linking) to link the user information to a uniquely identified individual in their databases[22,23]. Therefore, under current federal and provincial privacy legislation these data may be categorized as personal information (Box 1). Similarly, recent rulings in the European Union determined that these types of data are personal information under the GDPR[24,25].

Data collected from one source at one point in time may provide little information and be of little value to a data broker. However, with the data-matching methods, data brokers track users and collate data from multiple digital trails (e.g., smart phones, wearables, digital assistants, online browsing). Using this information, data brokers create a sophisticated picture of an individual's interests, influences, and behaviours. The aggregated data, particularly when sourced from healthcare queries or health-related services, can be processed by AI and can provide insights into an individual's mental and physical health[26–28]. This is often called "emergent medical data"[27,28]. Thus, through the accumulation of vast amounts of digital traces, data brokers gain insight into an individual's mental and physical health, which can be exploited for political or commercial gain[26-28].

If VCP companies, therefore, share user information with a data broker, they are disclosing health-related information about a uniquely-identified individual in a data brokers database. These profiles may be nameless, but contain enough other identifiers that the information can identify an individual[22,30]. The sharing of information may be particularly problematic if the platforms only provide one type of health service (e.g., mental health services or HIV prevention services) as they are revealing the nature of an individual's health concern. These user data, therefore, should be defined as PHI and companies should not share the information with third parties who conduct data matching[31]. As the VCP companies collect and share the information in the course of commercial activities, PIPEDA applies; to date, however, the OPC has not provided guidance on this issue.

DE-IDENTIFIED DATA

Finally, VCP company documents and interviews revealed that some companies create, use, and share de-identified health information. VCP companies appeared to view de-identified data as a proprietary asset that posed no privacy risks to patients. Studies show, however, that unless so much information is removed or manipulated that the data have little use, identification of some individuals is always possible[32]. Further, privacy loss is more likely to happen if data are widely shared with third parties and linked to other datasets[33–35]. Loss of privacy may lead to identity theft[35] and to blackmail[36].

De-identified data can also cause harm through other mechanisms. For example, remaining quasi-identifiers like partial postal codes or year of birth can be used to identify certain groups and make inferences about them[37,38]. The inferences are incorporated into algorithms that decide everything from allocation of health resources to offers of employment[37,39]. Individuals often have no ability to contest these automatic decision-making systems, and in fact are rarely informed that they are being used. The algorithms have also been shown to reflect and reinforce societal biases[37,40–42]. As these proprietary algorithms are used widely, they may end up creating more barriers for groups that are already marginalized.

Yet, de-identified information has few protections in Canada. PIPEDA does not state if implied or express consent (Box 1) is required to create a de-identified dataset, what rules must be followed during the de-identification process, nor what organizations can do with de-identified datasets. Commercial VCPs, therefore, can de-identify PHI without express patient consent, and without specifying data uses, to bring it outside the scope of the law. In Ontario, PHIPA permits health information custodians to de-identify PHI without patient consent as long as they provide transparency and ensure data security and confidentiality[43,44]. In Alberta, health data custodians are also permitted to "strip, encode or otherwise transform individually identifying health information to create non-identifying health information" without consent[45]. These legislations, therefore, remove patients' agency over their health information; without consent, their data can be de-identified and moved outside the scope of the law.

MONETIZING DATA, PROMOTING PHARMACEUTICAL PRODUCTS

Our analysis calls into question the narrative that the commercial virtual care industry creates more efficient models of care than the public sector. Rather, as depicted by participants, the commercial virtual care industry depends on monetizing patient data. Participants described how VCP companies used the data they collected to market other products, to conduct targeted advertising for third parties, and to assist in the creation of new products and services. Participants described these business uses of data as essential to the commercial VCP business model.

Of concern, some VCP companies analyzed and adjusted patient care pathways to optimize the uptake of a business partner's product. In examples provided by participants, pharmaceutical companies paid VCP companies to conduct analyses and adjust care pathways (e.g., timing of follow-up appointments, scheduling of laboratory tests, frequency of email reminders) to optimize uptake of a medication or vaccine. Although some participants framed these data-driven business ventures as win-win as they did not require the sharing of identified patient information, they present risks to patients. These activities may lead to care influenced by commercial interests, rather than focused on producing the best health outcomes. Research evidence supports this concern. Promoting pharmaceutical products does not improve health outcomes and may lead to harms by stimulating rapid uptake of a new drug before its risk profile is fully known[46]. Additionally, if platforms are not disclosing how they are using data to influence patient behaviour, patients are not able to meaningfully consent to these data uses. If platforms de-identify PHI prior to analyses, VCP companies may be able to legally conduct these analyses without informing patients under the relevant provincial or federal legislation. This is a substantial gap in legislation.

Activities that influence patient care pathways have drawn the attention of authorities in Canada and the US in the past. In 2017, pharmaceutical companies paid TELUS, a large Canadian corporation, to insert vouchers into its electronic medical record systems (used by thousands of physicians across Canada[47]) to promote the prescribing of their brand-name drugs, rather than competitors' generic drugs[48]. The voucher would cover any out-of-pocket cost for the patient if the insurer would only pay for the cheaper generic drug. The practice sparked outcry from doctors and concern from the Minister of Health that the practice might affect drug costs[48]. In 2021, Practice Fusion, an American electronic medical record vendor, had to pay $145 million in fines because it accepted payments from a pharmaceutical company to promote its products through the platform[49]. The US Deputy Assistant Attorney General stated, "Kickbacks from drug companies to software vendors that are designed to improperly influence the physician-patient relationship are unacceptable. When a software vendor claims to be providing unbiased medical information— especially information relating to the prescription of opioids — we expect honesty and candor to the physicians making treatment decisions based on that information"[49].

CONSENT

Although commercial VCPs seek consent before using data for these purposes, our analysis reveals multiple barriers to meaningful consent. First, individuals may not carefully evaluate privacy policies because they assume commercial VCPs collect and use their data only to provide clinical care. They may also not be in the frame of mind to evaluate policies when they are seeking urgent medical attention. Furthermore, many privacy policies use technical language and vague terminology that provides limited information. This lack of clarity may be due to complicated data flows within companies and externally with third parties (e.g., subcontractors, partners, affiliates, etc.). These vague policies make it difficult for a patient to understand where their data may be used or shared in the future.

Additionally, participants described how some commercial VCPs made it difficult, or impossible, for patients to opt-out of data collection and data uses (such as marketing and business development) that were not essential for the provision of the health care. Accordingly, if patients did not want to provide their information for the reasons listed in a privacy policy, platforms privacy policies informed patients that they may not be able to use all aspects of the health services or, in some cases, had to stop using the platform altogether. Platforms generally did inform patients in their privacy policies how to opt-out of certain trackers and how to opt-out of marketing messages.

A lack of jurisdictional clarity makes it difficult to determine if these practices are permitted. Canadian privacy legislation generally requires that a commercial VCP collect the least amount of information reasonably necessary to provide a service[44,50,51]. For example, if VCP companies are gathering these data for marketing purposes as organizations governed under PIPEDA, this information could be considered necessary to this business purpose[51]. However, if the commercial VCP is acting as an affiliate of a health custodian under Alberta's HIA, for instance, the collection of the information must be limited to that which is in accordance with the affiliate's duties to the custodian [50]. This lack of clarity creates a gap that commercial VCPs appear to be exploiting. Ensuring that provincial PHI legislation covers all the activities of commercial VCPs when they are providing health services would better protect patient privacy.

Whether these practices are legal or not, they raise the question of whether it is appropriate to require patients to consent to commercial uses of their data to access a provincially funded health service (or any health service). These practices also place an unfair burden on the 15 percent of people in Canada without a primary care provider[13]. They have fewer options when seeking healthcare and may feel they have no choice but to use these commercial services, services that put them at risk of privacy-related harms. Further, individuals without a regular care provider are more likely to be people who are new immigrants, homeless or under-housed; use substances, have addictions or receive opioids for chronic pain[52–54], all groups that face discrimination and barriers to care[55–58].

INDIGENOUS DATA SOVEREIGNTY

Furthermore, the datasets contain data from First Nations, Inuit, and Métis people in Canada, many of whom can be identified by postal code or geolocation codes. This necessitates that Indigenous-led Data Governance mechanisms be applied to ensure appropriate control, use, and benefit from the data by inherent Indigenous rights holders. Examples of Indigenous Data Governance mechanisms include the First Nation's Principles of Ownership, Control, Access, and Possession (OCAP®) and the international Collective benefit, Authority to Control, Responsibility, Ethics (CARE) Principles for Indigenous Data Governance [59, 60]. There is no one-size-fits-all approach to Indigenous Data Governance. Therefore, ensuring that Indigenous data are governed by appropriate Indigenous Nations requires meaningful engagement and consultation with Indigenous leadership to co-develop mechanisms that support Indigenous self-determination and autonomy. Without appropriate processes in place, these data have the potential to cause collective harm to communities[59, 60].

LOSS OF A PUBLIC GOOD

The expansion of commercial virtual care services may lead to a loss of a public and community asset – health data. Currently, many primary care clinics share the health data they collect with non-profit and public research networks across provinces. These research networks have ethics approval from public institutions to collect the data and use it for research and health system improvement. The networks have governance bodies to ensure the uses are in the public interest[61].

Our research indicates, however, that VCP companies may decline to share their data with these public and non-profit data repositories. Participants described how companies viewed data as a proprietary asset that lost value if shared with other entities. As a result, the proliferation of commercial VCPs may result in data silos where public and non-profit research organizations no longer have access to patient data for research and health system improvement. Research organizations have had difficulty in the past accessing health data held by other for-profit companies. In Canada in 2017, two major electronic medical record vendors blocked non-profit research networks from extracting data, saying the networks “could receive monthly data extractions for an additional fee, but could not choose what those extractions contained”[62]. Anything beyond that regular package would “cost extra” [62]. American research networks experienced similar issues with accessing health data[63]. As a result, the public may no longer see benefit from secondary uses of their collective health data[64].

CONCLUSIONS

Our analysis indicates that a lack of privacy protections, as well as legislative gaps and jurisdictional issues are putting individuals, marginalized groups, and society at risk of harms from commercial virtual care. Harms include exposure of sensitive health-related information and influence of patients' health care journeys to promote pharmaceutical and other products. Additionally, harms from these uses of data are likely to fall disproportionately on groups that are marginalized. Our analysis, therefore, highlights how privacy law serves a gatekeeper function that provides threshold protection for human rights, and protects group and communal interests[65].

Additional privacy protections and actions by regulatory bodies may reduce these risks (see recommendations). Further, if the commercial virtual care industry cannot survive without monetizing data in ways that expose people to harms, public or non-profit models may be more appropriate.

References

1.Personal Information Protection and Electronic Documents Act [PIPEDA]. Sect. SC 2000, c 5.
2. An Act respecting the protection of personal information in the private sector, R.S.Q., c. P-39.1; Organizations in the Province of Quebec Exemption Order, SOR/2003-374.
3. Personal Information Protection Act, SBC 2003, c 63; Organizations in the Province of British Columbia Exemption Order, SOR/2004-220;
4. Personal Information Protection Act, SA 2003, c P-6.5; Organizations in the Province of Alberta Exemption Order, SOR/2004-219.
5. Health Information Custodians in the Province of Ontario Exemption Order, SOR/2005-399.
6. Personal Health Information Custodians in New Brunswick Exemption Order, SOR/2011-265;
7. Personal Health Information Custodians in Newfoundland and Labrador Exemption Order, SI/2012-72.
8. Personal Health Information Act Exemption Order, SOR/2016-62.
9. Personal Health Information Protection Act (PHIPA) supra note _, s 2; HIA, supra note _, s 1(1)(a).
10. Personal Health Information Protection Act (PHIPA) supra note _, s 10.
11. Information and Privacy Commissioner of Ontario. Privacy and security considerations for virtual health care visits: Guidelines for the health sector. 2021. Available from: https://www.ipc.on.ca/wp-content/uploads/2021/02/virtual-health-care-visits.pdf
12. Office of the Information and Privacy Commissioner of Alberta. Investigation report H2021-IR-01: Investigation into the use of Babylon by TELUS Health by Alberta physicians (2021), online (pdf): Available from: https://www.oipc.ab.ca/media/1165671/h2021-ir-01.pdf [Babylon Telus Investigation].
13. Government of Canada SC. Primary health care providers, 2019. 22 Oct 2020 [cited 25 Mar 2022]. Available from: https://www150.statcan.gc.ca/n1/pub/82-625-x/2020001/article/00004-eng.htm
14. Canadian Institute for Health Information. How Canada Compares: Results From The Commonwealth Fund's 2016 International Health Policy Survey of Adults in 11 Countries — Accessible Report. CIHI; 2017. Available from: https://www.cihi.ca/sites/default/files/document/text-alternative-version-2016-cmwf-en-web.pdf
15. Lapointe-Shaw L, Salahub C, Bhatia RS, Desveaux L, Glazier RH, Hedden L, et al. Characteristics and healthcare use of patients attending virtual walk-in clinics: a cross-sectional analysis. medRxiv; 2022. p. 2022.02.28.22271640. doi:10.1101/2022.02.28.22271640
16.Canada O of the PC of. 2018-19 Survey of Canadians on Privacy. 9 May 2019 [cited 25 Mar 2022]. Available from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#fig10
17. Peekhaus W. Personal health information in Canada: A comparison of citizen expectations and legislation. Government Information Quarterly. 2008;25: 669–698. doi:10.1016/j.giq.2007.05.002
18. Madden M. Americans Consider Certain Kinds of Data to be More Sensitive than Others. In: Pew Research Center: Internet, Science & Tech [Internet]. 12 Nov 2014 [cited 25 Mar 2022]. Available from: https://www.pewresearch.org/internet/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/
19. Personal Information Protection and Electronic Documents Act, SC 2000, c 5 [PIPEDA], s 2(d) and (e).
20. Health Information Act, RSA 2000, c. 5, s1(1)k.
21. Canada O of the PC of. What an IP Address Can Reveal About You. 22 May 2013 [cited 15 Jan 2021]. Available from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/
22. Christl W, Spiekermann S. Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Facultas; 2016. Available from: http://crackedlabs.org/en/networksofcontrol https://www.dataprotectionreport.com/2022/02/european-rulings-on-the-use-of-google-analytics-and-how-it-may-affect-your-business/
23. Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Back on the Data Trail: The Evolution of Canada's Data Broker Industry. 2018. Available from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2017-2018/p_201718_04/
24. The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL). Decision [...] [...] ordering the company [...] to comply. 2020. Available from: https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf
25. NOYB European Centre for Digital Rights. Data Protection Complaint. 2020. Available from: https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt%20EN.pdf
26. Ebeling MFE. Healthcare and Big Data: Digital Specters and Phantom Objects. 1st ed. 2016 edition. New York: Palgrave Macmillan; 2016.
27. Marks M. Emergent Medical Data: Health Information Inferred by Artificial Intelligence. Rochester, NY: Social Science Research Network; 2020 Mar. Report No.: ID 3554118. Available from: https://papers.ssrn.com/abstract=3554118
28. Merchant RM, Asch DA, Crutchley P, Ungar LH, Guntuku SC, Eichstaedt JC, et al. Evaluating the predictability of medical conditions from social media posts. PLOS ONE. 2019;14: e0215476. doi:10.1371/journal.pone.0215476
29. Cadwalladr C, Graham-Harrison E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. 17 Mar 2018. Available from: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed 15 Jan 2021.
30. Zuiderveen Borgesius F. Singling Out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation. Rochester, NY: Social Science Research Network; 2016 Feb. Report No.: ID 2733115. doi:10.2139/ssrn.2733115
31. Personal Information Protection and Electronic Documents Act [PIPEDA]. principle 4.3.4.
32. Rocher L, Hendrickx JM, Montjoye Y-A de. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun. 2019;10: 1–9. doi:10.1038/s41467-019-10933-3
33. HealthITSecurity. 32M Patient Records Breached in First Half of 2019, 88% Caused by Hacking. In: HealthITSecurity [Internet]. 1 Aug 2019 [cited 19 Dec 2019]. Available from: https://healthitsecurity.com/news/32m-patient-records-breached-in-first-half-of-2019-88-caused-by-hacking
34. Eckert S, Dewes A. Dark Data. 2019 Jul 27; DefCon. Available: https://www.defcon.org/html/defcon-25/dc-25-speakers.html
35. O'Flaherty K. Why Cyber-Criminals Are Attacking Healthcare -- And How To Stop Them. In: Forbes [Internet]. Oct 2018 [cited 12 Sep 2019]. Available from: https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/

36. Guardian. “Shocking” hack of psychotherapy records in Finland affects thousands. In: the Guardian [Internet]. 26 Oct 2020 [cited 27 Oct 2020]. Available from: http://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland
37. O’Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. 1st edition. New York: Crown; 2016. doi:10.5860/crl.78.3.403
38. McBride K. Data Resources and Challenges for First Nations Communities Document Review and Position Paper Prepared for the Alberta First Nations Information Governance Centre [Internet]. Alberta First Nations Information Governance Centre; Available from: https://www.afnigc.ca/main/includes/media/pdf/digital%20reports/Data_Resources_Report.pdf
39. Office of the Privacy Commissioner of Canada. Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence. 28 Jan 2020 [cited 28 Jul 2020]. Available from: https://web.archive.org/web/20201112024158/https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/
40. Kemper J, Kolkman D. Transparent to whom? No algorithmic accountability without a critical audience. Information, Communication & Society. 2018;0: 1–16. doi:10.1080/1369118X.2018.1477967
41. Benjamin R. Assessing risk, automating racism. Science. 2019;366: 421–422. doi:10.1126/science.aaz3873
42. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366: 447–453. doi:10.1126/science.aax2342
43.Decisions PHIPA 175 [Internet]. IPC. [cited 2022 May 20]. Available from: https://decisions.ipc.on.ca/ipc-cipvp/phipa/en/item/520967/index.do?q=phipa+175
44. Personal Health Information Protection Act (PHIPA) s 37(1)(f)).
45. Health Information Act, s65.
46. Mintzes B. Should Canada allow direct-to-consumer advertising of prescription drugs? Can Fam Physician. 2009;55: 131–133.
47. Vendor Market Share [Internet]. [cited 2022 May 20]. Available from: https://wwwdev.nonprod.ontariomd.ca/emr-certification/certified-emrs/vendor-market-share
48. McLean J, Bruser D. Hoskins will ‘express concerns’ about patient record software being used to sell drugs. The Toronto Star. 3 Aug 2017. Available from: https://www.thestar.com/news/queenspark/2017/08/03/hoskins-will-express-concerns-about-patient-record-software-being-used-to-sell-drugs.html. Accessed 21 Dec 2021.
49. Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations. 27 Jan 2020 [cited 14 Feb 2020]. Available from: https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0
50. Health Information Act, s 24(b).
51. Personal Information Protection and Electronic Documents Act [PIPEDA], principle 4.4.
52. Hay C, Pacey M, Bains N, Ardal S. Understanding the Unattached Population in Ontario: Evidence from the Primary Care Access Survey (PCAS). Healthc Policy. 2010;6: 33–47. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3016634/
53. Spithoff S, Kiran T, Khuu W, Kahan M, Guan Q, Tadrous M, et al. Quality of primary care among individuals receiving treatment for opioid use disorder. Canadian Family Physician. 2019;65: 343–351. Available from: https://pubmed.ncbi.nlm.nih.gov/31088874/
54. Gomes T, Campbell TJ, Martins D, Paterson JM, Robertson L, Juurlink DN, et al. Inequities in access to primary care among opioid recipients in Ontario, Canada: A population-based cohort study. PLoS Med. 2021;18: e1003631. doi:10.1371/journal.pmed.1003631
55. Edge S, Newbold B. Discrimination and the health of immigrants and refugees: exploring Canada’s evidence base and directions for future research in newcomer receiving countries. J Immigr Minor Health. 2013;15: 141–148. doi:10.1007/s10903-012-9640-4
56. Rao H, Mahadevappa H, Pillay P, Sessay M, Abraham A, Luty J. A study of stigmatized attitudes towards people with mental health problems among health professionals. J Psychiatr Ment Health Nurs. 2009;16: 279–284. doi:10.1111/j.1365-2850.2008.01369.x
57. Urbanoski K, Pauly B, Inglis D, Cameron F, Haddad T, Phillips J, et al. Defining culturally safe primary care for people who use substances: a participatory concept mapping study. BMC Health Serv Res. 2020;20: 1060. doi:10.1186/s12913-020-05915-x
58. Kennedy-Hendricks A, Barry CL, Gollust SE, Ensminger ME, Chisolm MS, McGinty EE. Social Stigma Toward Persons With Prescription Opioid Use Disorder: Associations With Public Support for Punitive and Public Health-Oriented Policies. Psychiatry Services. 2017;68: 462–469. doi:10.1176/appi.ps.201600056
59. FNIGC / CGIPN. A First Nations Data Governance Strategy [Internet]. 2020 [cited 2020 Nov 30]. Available from: https://fnigc.inlibro.net/cgi-bin/koha/opac-retrieve-file.pl?id=9c677f3dcf8adbf18fcda96c6244c459
60. Carroll SR, Garba I, Figueroa-Rodríguez OL, Holbrook J, Lovett R, Materechera S, et al. The CARE Principles for Indigenous Data Governance. Data Science Journal. 2020 Nov 4;19(1):43. doi:10.5334/dsj-2020-043
61. FNIGC / CGIPN. Ownership, Control, Access and Possession (OCAPTM): The Path to First Nations Information Governance. 2014. Available from: https://web.archive.org/web/20200909011418/https://fnigc.ca/sites/default/files/docs/ocap_path_to_fn_information_governance_en_final.pdf
62. Owens B. Family doctors call for guaranteed access to EMR data for research and quality improvement. CMAJ. 2018;190: E60–E61. doi:10.1503/cmaj.109-5543
63. Tahir D. Specialty societies say EHR vendors are blocking their registry work. In: POLITICO [Internet]. 2016 [cited 9 Jun 2020]. Available from: http://politi.co/2hdcVxZ
64. Mandl KD, Kohane IS. Data Citizenship under the 21st Century Cures Act. New England Journal of Medicine. 2020;382: 1781–1783. doi:10.1056/NEJMp1917640
65. Regan P. Privacy as a Common Good in the Digital World. Information. 2002;Communication&Society: 382–405. doi:10.1080/13691180210159328

SECTION 7: RECOMMENDATIONS

JURISDICTION, DATA PROTECTIONS

To address risks to privacy, we recommend that policymakers provide clarity on jurisdiction over commercial VCPs. Additionally, policymakers should update federal private sector legislation to provide enhanced protections to PHI. This would ensure that when the activities of commercial VCPs do not fall under provincial privacy legislation, PHI still receives the same degree of protections. Policymakers should also bring de-identified information within the scope of the law to give it appropriate protections that reflect the sensitivity of the data. Finally, provincial and federal policymakers should ensure that all new and updated legislation recognizes Indigenous Peoples' inherent rights to sovereignty, inclusive of Indigenous data sovereignty.

DATA DEFINITIONS

We recommend that federal and provincial regulators issue clear guidance around the categorization of data collected by commercial VCPs. In particular, we recommend that registration and sign-up information (e.g., names, email addresses, etc.) and other personal information collected by the platforms are clearly defined as PHI. We also recommend provincial and federal regulators provide clear guidance concerning user data (e.g., IP address, location information, cookie data) that commercial VCPs collect when individuals access these services. As these user data are from a platform that provides health services, contain identifiers and can often be data-matched to a uniquely identified individual, they should also be defined as PHI.

CONSENT

Policymakers and regulators should ensure that patients are able to access a health service without having to consent to the collection, use and sharing of their personal information and de-identified health information for commercial reasons. Patients are in a vulnerable position when seeking care, and the data they provide are sensitive. To collect and use data for purposes other than the provision of a health service, commercial VCPs should seek explicit, opt-in consent for each type of data use (e.g., marketing, business development, de-identification, etc.) in a way that does not impair, interfere with, or delay a patient's access to care. Regulators should also prohibit data-matching (i.e., linking a website user's information to a unique profile of an individual using identifiers like IP address) by the commercial VCPs and third parties. Finally, to further ensure that consent is valid, regulators should require commercial VCPs to share, in real-time, all third parties to whom they disclose personal information and de-identified health information.

DATA USES

We recommend that policymakers prohibit commercial VCPs from adjusting and influencing patient care pathways to increase uptake of pharmaceutical products, like medications or vaccines. Further they should prohibit all pharmaceutical promotion, including sponsored disease awareness, product placement and drug-related messaging.

OVERSIGHT AND MONITORING

We also recommend that privacy regulators conduct regular audits and investigations of commercial VCPs to ensure adherence to privacy legislation and regulation. Governments should provide privacy regulators with the appropriate resources to conduct these activities. Indigenous organizations should also have the authority to audit and investigate any uses of their data and be meaningfully informed throughout all uses and processing of Indigenous data. Additionally, professional medical regulatory bodies should provide guidance to and oversight of members (e.g., physicians and nurse practitioners) who provide care through commercial VCPs to ensure they are adhering to privacy legislation and regulation. We recommend the regulatory bodies implement practices to ensure patient well being is prioritized when their members use these platforms.

HEALTH SYSTEMS

With respect to the health systems, policymakers should require commercial VCPs to share their data, when appropriate, with designated public entities and with First Nations, Inuit, and Métis-identified Indigenous organizations for research and health system improvement. Governments should create infrastructure to facilitate data-sharing and should enforce stringent data protections. Provincial health systems should ensure that all patients have access to a primary care provider and create mechanisms to promote the integration of virtual care into ongoing care.

Table 4: Recommendations

	Recommendations	Mechanism
Jurisdiction, data protections	1. Clarify jurisdiction over commercial VCPs and their activities	Regulatory guidance
	2. Heighten privacy protections for PHI under PIPEDA, so that all collection, use and disclosure of PHI is governed under a similar standard, notwithstanding the nature of activities.	Amendments to PIPEDA
	3. Include de-identified information within the scope of federal and provincial legislation and provide data protections that reflect the sensitivity of the information.	Amendments to PIPEDA and provincial legislations
	4. Ensure all updated and new legislation recognizes Indigenous Data Sovereignty.	Amendments to PIPEDA and provincial legislations
Data definitions	5. Categorize all personal information collected when individuals access commercial VCPs as PHI.	Regulatory guidance or amendments to PIPEDA and provincial legislations
Consent	6. Ensure that VCPs permit individuals to access health services without having to consent to commercial uses of their personal information and de-identified health information.	Amendments to PIPEDA and provincial legislations
	7. Ensure commercial VCPs seek explicit opt-in consent for any commercial uses of personal information and de-identified information.	Regulatory guidance or amendments to PIPEDA
	8. Ensure that these processes to seek consent for commercial uses do not impair, interfere with or delay a patient's access to health services.	Regulatory guidance or amendments to PIPEDA
	9. Prohibit commercial VCPs from data-matching information. VCPs should be mandated to include a data-matching prohibiting clause in their sharing agreements with third-parties.	Regulatory guidance or amendments to PIPEDA and provincial legislations
	10. Require commercial VCPs to disclose all third parties with whom they share personal information or de-identified information in real-time.	Regulatory guidance
Data uses	11. Prohibit commercial VCPs from influencing patient care pathways to promote pharmaceutical products.	Regulatory guidance or amendments to PIPEDA and provincial legislations
	12. Prohibit all pharmaceutical promotion, including sponsored disease awareness, product placement and drug-related messaging.	Regulatory guidance or amendments to PIPEDA and provincial legislations
Oversight and monitoring	13. Conduct regular audits of commercial VCPs to assess for compliance with privacy legislation and regulation.	Enhanced regulation
	14. Ensure that physicians and nurse practitioners who provide health care services through commercial VCPs adhere to their responsibilities to protect patient information.	Professional regulatory bodies

Table 4: Recommendations Continued

	Recommendations	Mechanism
Health systems	15. Require commercial VCPs to share de-identified health information with public entities and Indigenous organizations for research and health system improvement, when appropriate.	Regulatory guidance or amendments to legislation
	16. Create mechanisms to support integration of virtual care into patients' ongoing care with a regular care provider.	Provincial health care policies and practices
	17. Ensure all Canadians have access to a regular primary care provider.	Provincial health care policies and practices

PHI = Personal Health Information; PIPEDA = Personal Information Protection and Electronic Documents Act; VCP = Virtual Care Platform

APPENDIX

Acronyms

Acronym	Full Term
ADS	Automated-Decision System
AI	Artificial Intelligence
CESP	Consumer Electronic Service Providers
GDPR	General Data Protection Regulation
GIC	Governor in Council
HINP	Health Information Network Provider
HIA	Health Information Act *(Alberta)*
IP	Internet Protocol
IT	Information Technology
OIPC	The Office of the Information and Privacy Commissioner
OPC	The Office of the Privacy Commissioner of Canada
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act *(Ontario)*
PIPA	Personal Information Protection Act *(Alberta)*
PIPEDA	Personal Information Protection and Electronic Documents Act *(federal)*
VCP	Virtual Care Platform